CONCEALING ATROCITY CRIMES WITH OFFICIAL SECRECY: "NATIONAL SECURITY" AS A THREAT TO INTERNATIONAL SECURITY

Christopher Elliott

Submission Date: 18 September 2025; Acceptance Date: 25 November 2025; Publication Date: 23 June 2026

Copyright: © 2026, Christopher Elliott. This is an open-access article distributed under the terms of the Creative Commons Attribution Licence (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.

Abstract: This article uses a comparative history method to examine criminal state secrecy in closed authoritarian societies and open democratic societies. Focusing on how government secrecy is employed to conceal atrocity crimes, this article compares the legal, policy, and normative tools that state actors use to hide inhumane conduct and escape accountability for serious violations of international law. Observed outcomes for atrocity whistleblowers and the international criminal justice process are also examined. In describing the deleterious impact that secrecy can have for international justice efforts, this article proposes that the invocation of "national security" in war crimes, crimes against humanity, and genocide cases is in foundational tension with species-level international security concerns.

Keywords: State secrecy; atrocity crimes; whistleblowing; international security; political repression

DOI: 10.13169/statecrime.15.1.0002

Introduction

On 14 May 2024, former Australian Defence Force (ADF) lawyer David McBride walked into a Canberra courtroom to learn that he would be spending the next five years in jail. Jarring though the verdict was, his predicament had been some years in the making, having begun with his 2016 decision to disclose more than 200

Anthropologist and War Crimes Researcher, British Columbia Institute of Technology, Canada
Email: cgaelliott@gmail.com
ORCID: 0009-0002-9577-7666

military documents to journalists (R v McBride 2024). Most of the documents contained information the ADF considered "classified" – meaning that for reasons of "national security" they must not be transmitted, without authorization, outside government channels.

Despite their supposedly "secret"[1] nature however, when journalists took hold of the documents, a hefty selection formed the basis of *The Afghan Files*, a seven-part investigative series which unveiled, for the first time and in fastidious detail, a years-long pattern of war crimes by Australian special forces in Afghanistan (ABC 2017).

Beyond the crimes themselves, the McBride case sparked a wider controversy in Australian society about the proper role, and indeed the potential for abuse, of official secret-keeping.[2] How, some commentators asked, can the state charge, convict, and jail a soldier for revealing crimes committed by the very state doing the prosecuting (ABC 2024, Pender and Greste 2024)? Was prejudice to "the defence, national security or international relations of Australia" really the most important harm here, as the government claimed? Was "national security" actually the injured party? Framed another way, wasn't it much more egregious that the Australian government had committed these atrocities in the first place? And wasn't it even more egregious that official secrecy had concealed these crimes from public view until journalists took custody of and "illegally" published the material?

Since the end of World War II, a peremptory norm in the international system considers some crimes to be so atrocious that they shock the conscience of humanity and "threaten the peace, security and well-being of the world" (Office of the High Commission for Human Rights 1998). By logical extension, atrocity crimes[3] transcend "national security" concerns because, as a species-level threat, they harm *inter*national security – being the security of the entire international community of states. With this axiom front of mind, this article examines how states have used and abused official secrecy to conceal atrocity crimes in different societal settings. Examining the phenomenon of *criminal secrecy*[4] in government, this article will also describe a fundamental incompatibility between how states balance "national security" and "international security" interests in the practice of statecraft. Far from an abstract concern, this article will argue that this tension constitutes a foundational problem for the international legal order and undermines efforts to reduce atrocities worldwide.

In Part 1, this article will examine the political function and ethics of secret-keeping in various organizational contexts, both state and non-state. It will also examine the moral case for whistleblowing, as well as its moral limits.

In Part 2, this article will use a comparative history method to compare and contrast practices of criminal secrecy in "closed societies" and "open societies",

specifically in the context of atrocity crimes. In describing the mechanics of these practices, this article will examine the laws and policies that underlie state secrecy and the relevant bureaucratic praxes for "classifying" official information.

Literature Review

The Political Function of Secrecy

The practice of keeping secrets emerged in human society for many reasons, including to protect oneself from embarrassment; to preserve family honour; and to gain strategic advantage against competitors (Teft 1980: 14–17). While each of these reasons is socially distinct, they rest on a shared, functional assumption that disclosing information outside a given circle of knowledge has the potential to harm an interest, be it individual (in the case of private information) or group (in the case of a collective confidence).

That every secret is imbued with an "always to-be-guarded pathos" means that secrecy practices have shaped human organizational behaviour in fundamental ways, encircling secret-holders "like a boundary" (Simmel 1906: 484), regulating "what is and is not said by whom and to whom" (Costas and Grey 2014: 1424). The selective nature of secrecy – in which "a second world" (Simmel 1906: 462) of revealed knowledge co-exists alongside an ignorant one – also instils a politics into its practice because the secret-guardian's control over information necessarily confers power upon them (Manderson et al. 2015: s184).

The oft-remarked relationship between knowledge and power – encapsulated by the pithy claim that "knowledge *is* power" – appears to have a strong cross-cultural basis. In American Pueblo society, Brandt describes how the "inhibition of information flow" (Brandt 1980: 126) was an essential basis for the power wielded by the "Old People" (*lulina*). Of particular note, restricting access to mystical knowledge created status hierarchies which enhanced elders' prestige, thereby legitimizing their involvement in secular politics. In the resulting gerontocratic system, uninitiated youngsters (*oysemayana*) were "ceremonially poor" and therefore disenfranchised, despite their physical advantages (Brandt 1980: 137–142).

Among the Mekranoti of Central Brazil, Werner identifies a similarly strong correlation between the accumulation of socio-cultural knowledge and the amount of influence that older men wield over their community (Werner 1981: 19–21). Besides obtaining knowledge, keeping others *away* from it is equally critical for maintaining these systems. In this regard, Hiatt sees an explicitly gendered power dynamic in aboriginal Australia, where the "aggressive secrecy" of male-exclusive pseudo-reproductive rituals extends male domination into spheres where women have "evident" natural advantages (Hiatt 1971: 77–80).

The Legitimacy of Secrecy

Adjacent to the anthropological literature on secrecy is an overlapping philosophical debate about its moral appropriateness. In contemplations on the ideal forms of government, the legitimacy of secret-keeping is frequently contested, with statist thinkers often positioned against liberal and anarchist counterparts. Advocating for repressive censorship, Plato reasoned that a ruler should suppress information in furtherance of "the public good" (Plato 1991: 86–87), telling lies if necessary.[5] Arguing similarly, the 16th-century jurist Arnoldus Clapmarius proposed that the ruler must hold, as a matter of necessity, "certain deep and intimate" privileges over information (*arcana imperii*)[6] to advance the "public good" and to guard against faith-violating "atrocities" (*flagitia*) (Clapmarius 1644: 31). Clapmarius linked the *arcana* privilege to the "reason of state" (*ragnio di stato*) and the accompanying "right of domination" (*jura dominationis*) – the "undeservedly flogged" notion that the state may exercise power when legal means are insufficient (Clapmarius 1644: 23–24).[7]

Opposing absolutist visions of government, Botero condemned the secret plotting of illegalities by governments, arguing that a ruler must not "close the door of his privy council" and "follow a reason of state contrary to the law of God" (Botero 2017: 63).

Observing that state secrecy often "opens a space" for unfettered violence and oppression, Horn links the modern logic of political secrecy to ideas of state exceptionality previously developed by the Nazi jurist Carl Schmitt, who argued that a sovereign's limits "cannot be circumscribed factually and made to conform to preformed law" (Schmitt 1985: 6; Horn 2011: 103).[8]

An even more scathing critique of Plato's vision of totalitarian secrecy is seen in Karl Popper's *The Open Society and Its Enemies*, in which he characterizes Plato's idealized republic as an unjust, change-arrestive, anti-humanitarian system defined by caste rule and institutional opposition to free inquiry (Popper 1994: 101, 165–173). Militating against systems defined by "lying, political miracles, tabooistic superstition, the suppression of truth and, ultimately, brutal violence" (Popper 1994: 189), Popper marshals the liberalism of Socrates' "gadfly" – the "arousing and persuading and reproaching" nuisance, that, through uncensored critique, ensures that the public does not fall asleep (Popper 1994: 183–184).

With the expansion of bureaucratized state secrecy in the 20th century, an extension of this debate continues to play out in relation to so-called "leaks" of classified information. On one end of the debate, governments defend secret-keeping for reasons of "national security". Specifically, secrecy is described as necessary to preserve "equities" – to use a term that is in-vogue within Western intelligence bureaucracies (Office of the Director of National Intelligence 2016: 4). In the context of government intelligence operations, "equities" typically refer

to vulnerable "sources and methods" – for example, human intelligence sources (whose lives may be endangered if their identities are exposed) and signals intelligence collection methods (which are susceptible to adversary technical countermeasures). Other vulnerable "equities" may include the current locations of sensitively disposed military or intelligence personnel, whose lives could be threatened if compromised. More banally, other information over which the state often claims a secrecy privilege includes the personal tax information and medical information of citizens.

On the opposite end of the modern secrecy debate are the denizens of the digital age counter-revolution against closed government. Thinkers within this group propose overturning official secrecy altogether, arguing that "radical transparency" is the only way to ensure that governments are operating in the public's best interest (Brevini 2017). The Wikileaks organization is the most renowned actor in this camp, with its unexpurgated approach exemplified by extreme actions such as publishing the personally identifying information of Afghan informants linked to the US military (CBC 2010).

Reviewing this debate, Sagar portrays state secrecy as something of an intractable "dilemma". On the one hand, he notes, a government concealing its activities from the public is antithetical to democracy. On the other hand, secrecy is evidently sometimes necessary, since among the masses of state-held information, governments reposit material whose unauthorized disclosure would cause serious harm. Painting the Wikileaks perspective as a reckless outlier, Sagar argues that the issue is not whether genuine "national security" justifications for secrecy exist. Instead, the thornier question revolves around how national security suppression is applied and who has control over the contours and limits of its application. As he writes: "[It] is not about the legitimacy of secrecy *per se*, but rather about ensuring that state secrecy is used only to further national security" (Sagar 2023: 3).

Informal Secrecy and Whistleblowing

While there are evidently legitimate reasons for governments to keep secrets, certain forms of secrecy are undoubtedly harmful. Here, Costas and Grey make a distinction between the risks associated with "formal secrecy" (whose limits are defined by reviewable systems of rules) and "informal secrecy", its *un*regulated opposite which lacks a legal basis and is "organized through social norms" (Costas and Grey 2014: 1424).

Informal secrecy exists in many organizational settings, both state and non-state. In organized crime settings, Sicilian Mafia groups have long maintained a code of silence called *omertà*, under which "made" members of the enterprise pledge never to provide information to state authorities (Paoli 2003: 109). Being a tight-knit, closed-circle social system, betrayal of this oath is considered a fatal

mark of dishonour such that those who become *pentiti* ("repentants") and turn state witness may be subjected to retaliation.[9] An analogous rule within American street gangs is articulated in the well-known adage that "rats" or "snitches" can expect to "get stitches" (National Center for Victims of Crime 2007, Westmarland 2013).

In other criminal settings, informal "codes" that enforce a knowing-yet-complicit silence may be implied rather than explicitly stated, often hinging on collective understandings that outside-the-circle disclosure will be mutually destructive to every member of the group. This is commonly the case with corporate malfeasance, where cover-ups of financial and environmental crimes are aimed at preventing contract losses and lay-offs (Beamish 2000).[10]

Ethnographic studies of criminality within law enforcement communities have similarly remarked on the so-called "blue wall of silence" (Westmarland and Conway 2020) whereby an occupational propensity for secrecy and solidarity within policing organizations creates conditions where individuals are often reticent to report corrupt peer conduct (Kleinig 2001). In such conditions, anti-corruption reform requires direct intervention. Such interventions are often assisted by "whistleblowing", defined by DeMaria as "an individualistic minority response to wrongdoing" (Demaria 2006: 219).

A classic illustration of whistleblowing is seen in Detective Frank Serpico's disclosures about the New York Police Department (NYPD) in the early 1970s. After witnessing colleagues engaged in bribery, racketeering, and selective enforcement during rounds as a plain-clothes officer, Serpico encountered further systemic issues within the NYPD when he attempted to report it. During one attempt to report corrupt conduct, an internal affairs investigator told Serpico that "by the time this thing is through, you'll be found floating in the East River, face down. Or you can just forget the whole thing". Eventually, Serpico's inability to obtain a satisfactory resolution internally culminated in an unauthorized disclosure to *The New York Times*, whose front page ran details about the crimes in April 1970 (*New York Times* 1970, Burnham 1970).

With near universality, Serpico's decision to breach departmental secrecy by talking to the *Times* is now regarded as a legitimate exercise of individual moral reasoning. The beneficial impact of his disclosures is especially palpable in the fact that a subsequent commission of inquiry substantiated his corruption allegations, leading to institution-wide reform within the NYPD.

While Serpico's actions are now considered uncontroversial, other examples of whistleblowing have provoked more nuanced debates about the moral limits of such disclosure. If it is true, for example, that keeping secrets is sometimes legitimate, what course of action should whistleblowers take when genuinely sensitive information will be collaterally disclosed alongside corrupt or criminal activity?

In distinguishing between disclosures of conscience and reckless breaches of confidentiality, some observers differentiate between "whistleblowing" and "leaking".

A Rorschach Test for this distinction is seen in the highly publicized disclosures of classified information by the US Army intelligence analyst Chelsea Manning. On the one hand, Manning's defenders style her a "whistleblower", pointing to specific revelations in her "war logs" data-dump that indicated illegal activity (Cadwalladr 2018). Within the Manning-provided material, the "Collateral Murder" video – which depicted the killing of two *Reuters* journalists by a US Apache helicopter in Iraq – is often regarded as disclosure-worthy information. The same can be said of another report which recounted the revenge killing of six Afghan civilians in the village of Nangar Khel by Polish paratroopers (*The Guardian* 2010).

Vastly outnumbering this incriminating material however, Manning's critics note that the sheer scale of her disclosures compromised untold other government activities, many of which fell well within the range of reasonable state behaviour.

Moreover, the method by which these disclosures were actuated also included attempts to crack passwords on a military computer network (Bump 2019) – an action that, if successful, could plausibly have resulted in false accusations being laid against another user. This conduct more closely resembles humdrum hacking activity – conduct which governments would ordinarily be expected to prosecute. Further, the claim that Manning was only interested in crimes quickly collapses when one considers the size of her disclosure – 750,000 files (Cadwalladr 2018). Even though some atrocity crimes were suffused throughout these files, the fact that the Taliban was able to use the more-banal logs to identify Afghans leaking the *Taliban's* secrets suggests an element of recklessness was imbued in these actions.

Flawed messengers though whistleblowers sometimes are, the ethical heart of the Chelsea Manning debate perhaps rests on a counterfactual. Would her disclosures have been legitimate had she *only* revealed illegal activities – say the "Collateral Murder" video and the Nangar Khel massacre – and nothing else? Although the inescapable answer to this question seems to be "yes", it is probable that the state would still have prosecuted her for breaching American secrecy laws. This, in turn, raises broader, under-studied questions about the specific secrecy tools (to include norm-, policy-, or law-based tools) that governments use to conceal atrocities from the public.

Data and Methods

In the following comparative history, this article will systematically examine the criminal abuse of official secrecy, drawing on case studies from eight states (Nazi

Germany, Myanmar, the Russian Federation, Australia, New Zealand, Canada, the United Kingdom, and the United States of America). After reviewing the secrecy laws and policies associated with these states, each case was coded as either a "closed society" (associated with *totalitarian secrecy*) or an "open society" (associated with *limited secrecy*).[11] Next, to understand how criminal secrecy operates in each type of society, three additional characteristics were examined – *methods of atrocity concealment*; *whistleblower outcomes*; and *international justice outcomes*.

Primary source data included relevant laws and policies as well as court documents. Other data sources included archival materials; biographies of key personalities; social media publications; and news reporting associated with court proceedings and other key events.

As will be shown, noteworthy in the results are the multifarious means by which official secrecy is abused, such that it is a powerful tool for concealing grave breaches of international law. Although the specific methods for concealing atrocities vary between society types, the outcomes for international justice are largely the same – being reproducible in a range of social, cultural, and historical contexts.

Collectively, the observed historical patterns also show that when left unchecked, abusive secrecy can even be a *facilitator* and *actuator* for atrocity – both as an active frustrater of justice and as a tool enabling further offending. Pertinently, criminal secrecy threatens international security by acting as:

1.) an obstructor of atrocity investigations and proceedings (*process frustration*);
2.) an actuator for continued offending (*perpetrator enablement*); and
3.) a deterrent against atrocity disclosure (*whistleblower deterrence*).

See Figure 1.

A Comparative History of Criminal State Secrecy

Criminal Secrecy in Closed Societies

In closed, authoritarian systems, the relationship between citizen and state is defined by a hierarchical ordering that is both "co-ordinate and subordinate" (Bergson 1935: 26).[12]

In these settings, the state claims an absolute sovereign right over all information circulating across society and within its own bureaucracy. Formally and in practice, this includes a right to *curate* informational content (by, for example, steering the editorial direction of state media) and a right to actively *censor*

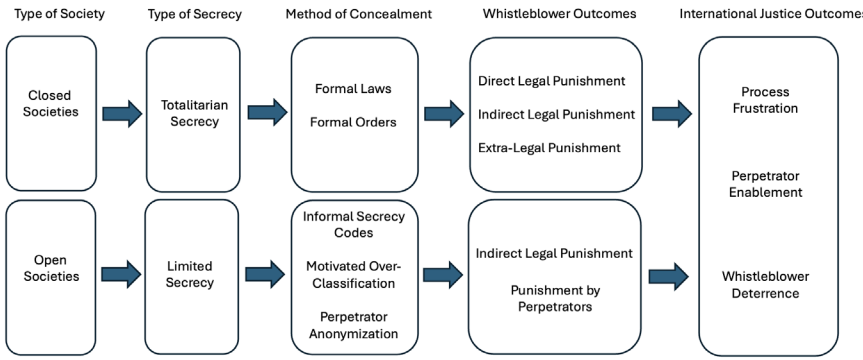

Figure 1. *State Concealment of Atrocity Crimes: Means, Methods and Outcomes*

content, as it flows in and out of the system. By default, information originating from within authoritarian government departments is aggressively vetted before reaching the masses. If the content is embarrassing to or criminally inculpates the state (by, for example, exposing a Tiananmen Square-like episode),[13] that information will be concealed *in toto*. Accordingly, the individual citizen has no inherent right to access state-originating information. In a closed society, the "right to know" does not exist.

When authoritarian officials assess that a particular item of information broaches upon a genuinely sensitive military or intelligence concern, such "official secrets" are even more tightly controlled, through the security classification system. Sequestered thus, the non-disclosure of state secrets is aggressively enforced across *all* spheres of society, without limitation. As we will see later, this is not the case in open societies, where prevailing norms evince at least some safeguards for media reporting on "leaks".

Accordingly, in systems of *totalitarian secrecy*, the primary tools for concealing atrocity are *formal laws* and *formal orders*. Both tools underwrite the state's absolute right to secrecy and its absolute authority over the citizen. In such systems, outcomes for whistleblowers (whether a government employee or a member of civil society) usually involve one of the following: 1.) *direct legal punishment*; 2.) *indirect legal punishment*; and/or 3.) *extra-legal punishment.* Using case studies from Nazi Germany, Myanmar and Russia, the mechanics of criminal secrecy in a closed society are described below.

Nazi Germany

The paradigm example of the use of state secrecy to conceal atrocity is the seen in the bureaucratic practices of the Third Reich. In Nazi Germany, official secrecy

was framed around Adolf Hitler's "Fundamental Order 1" (herein, the Secrecy Order), which began with the following absolute diktat:

> *No person, no agency, no officer is to obtain knowledge of a secret matter if it is not imperative for him to have knowledge because of official reasons…careless passing of orders whose secrecy is of decisive importance is prohibited* (Nuremberg Military Trial 4 1947: 2342).

As an articulation of the "need-to-know" principle, Hitler's Secrecy Order would be superficially familiar to anyone with professional experience in any government bureaucracy. If a government official does not need to know a secret fact, they generally are not informed of it.

With this "fundamental" principle in mind, information in the Third Reich was categorized in a highly systematic fashion, as reflected in an extremely well-defined scheme of security classification markings. Depending on its sensitivity, classified information could be "Confidential", "Secret" (*Geheime*), "Top Secret", or "Super Top Secret" (Nuremberg Military Trial 7 1947: 3770). Exceptionally sensitive information could also be consigned to an above-top secret compartment called "Secret Command Matter" (*Geheime Kommandosache*), which indicated that access to the information was "limited to a circle of persons which was directly connected with it" (Nuremberg Military Trial 4 1947: 1609)[14] *Kommandosache* documents were typically the privy of select leaders involved in early-stage preparations of a major operation. Such was the case with the classification markings on the Aktion Reinhardt Order, which triggered the deadliest phase of the Holocaust (Nuremberg Military Trial 7 1947: 3932).

Importantly, Hitler's Fundamental Order 1 did not explicitly prohibit using the security classification system to conceal atrocity crimes. Plainly, the opposite was the case because in the politico-legal system of Nazi Germany, an order originating from the Führer carried the total force of German domestic law, even if that order was manifestly criminal or contravened an international treaty.

One example of an internationally unlawful order that was still sequestered by the Third Reich's secrecy provisions is Hitler's *Geheime*-classified Commando Order (*Kommandobefehl*). This order instructed German troops to summarily execute allied commandoes found in German rear areas, in direct contravention of the 1907 Hague Convention (Nuremberg Military Trial 7 1947: 4697). Hitler's decision to issue this order was, of course, an international crime, and it became a centrepiece exhibit in the 1947 Nuremberg Military Trials. Nevertheless, in the context of the Third Reich's *domestic* legal regime, a German soldier was still bound to obey it (famously, the superior orders defence was never accepted as a legitimate defence at Nuremberg).

The "*Geheime*" security classification affixed to the Commando Order also carried with it an important yet often-overlooked obligation for its reader. By logical consequence of the "fundamental" principle in Hitler's Secrecy Order, a recipient soldier was not only bound to obey the Commando Order, he was also bound to keep the order's contents *secret* from uninitiated persons. Thus, a German soldier had two tasks when responding to *Kommandobefehl*: 1.) a duty to summarily execute prisoners; and 2.) an attendant duty to keep quiet about his reasons for having done so, since the existence of the Commando Order was a state secret. In other words, the German soldier's domestic duty under the laws of the Third Reich was to commit an international crime and then to keep the orders authorizing that crime a secret.

The sequestering effect of this information security framework was so profound that some of the Holocaust's worst crimes (including the use of gas chambers at the death camps) occurred in extraordinarily effective conditions of secrecy. In the main, the Nazi need-to-know principle was effectively upheld across the state because those involved in the killings took their non-disclosure obligations seriously (Breitman 1996: 71–72). This carefully compartmented legal secrecy was also reflected in the geometric design of the death camps themselves, where each step between the "reception area" and the "annihilation area" was blocked off by a series of high fences (Sofsky 1993: 260). As Sofsky writes:

> Only after space was sealed off totally, hermetically, did the camp become that closed locus where absolute power could unfold freely… The boundary line shielded the camp from the outside world, transforming it into a secret site of crime… The prisoner was forever removed from the protective sight of the public domain (1993: 55).

In some cases, secrecy (and one's willingness to abide by it) was also integral to the perpetrator's continuing participation in Nazi crimes. Reflecting on his involvement in the Aktion T4 euthanasia programme (where gassing technology was first tested), Franz Stangl asserted, not unconvincingly, that he never disclosed the mass murder campaign to his wife because it was a blanket-classified state secret (Sereny 1974: 78). Since his wife was a devout Catholic who might have objected had she known the details, Stangl's hassle-free participation in the programme thus depended on his being able to keep the murderous facts from his spouse. In other words, his doleful compliance with his secrecy obligations became an indispensable part of his ultimate "descent" into evil.

Later, when Stangl became the commandant of the Treblinka extermination camp, he *did* reveal the facility's function to his wife, reluctantly, in a presumed breach of his Secrecy Order obligations. He disclosed the truth not because he had

ceased taking those obligations seriously but because the smell from the camp was impossible to dismiss. Through persistent badgering, his wife had extracted the information. As Sereny quotes Frau Stangl:

> I knew after a while what he was doing. He wasn't supposed to say, of course, but you know how women are…I probed and probed and finally he told me. It was awful of course, but what could we do? (1974:106)

Despite ultimately succumbing to his wife's harrying, Stangl's years-long, obdurate fealty to Hitler's Secrecy Order demonstrates the importance of information security in the operational security of the Holocaust. Alongside related planning decisions – such as the decision to construct the death camps in geometrically particular ways, in secluded forested areas – Hitler's broad trust in subordinate confidentiality was central to the workability of the whole system. As Sereny notes, the "spreading of information" outside formally regulated channels constituted a "very real danger" to Hitler's objectives, so it was aggressively suppressed. Where knowledge about the extermination camps did escape, it seems to have been the exception, and not attributable to a widespread culture of leaking.[15]

Myanmar

If Nazi Germany archetypally illustrates how closed societies conceive official secrecy obligations (as a total onus upon the initiate, with no exceptions, even for atrocity crimes), modern states like Myanmar and Russia illustrate how such governments respond to the unauthorized disclosure of state-orchestrated atrocities. Two methods are employed when punishing these disclosures – *legal punishment* (either *directly* or *indirectly* through the criminal justice system) and *extra-legal punishment* (involving targeted harassment and extrajudicial killings).

In Myanmar, a prominent example of legal punishment is seen in the prosecution of two Reuters journalists following their reporting about the September 2017 Inn Din massacre. In October 2017, the journalists Wa Lone and Kyaw Soe began investigating the massacre in person, attending grave sites and photographing human remains (Lone et al. 2018). In November 2017, after concluding that police paramilitaries were responsible for the killings, Lone conducted follow-up interviews with members of the 8th Security Police Battalion (Reuters 2018). After senior Myanmar security forces officers got word of their inquiries, the journalists' police sources were arrested on suspicion of violating the Police Disciplinary Act, which prohibits unauthorized disclosures of police information (Reuters 2018). With the journalists' police sources captured, a Myanmar Brigadier then directed a subordinate to pass "secret" (ဝှက်ချက်) documents to Lone during a restaurant meet (a rather ordinary case of entrapment). Shortly after the document

exchange, both Lone and Soe were arrested for possessing classified information "with the intention to share it with foreign media" (Naing and Slodkowski 2018; Al-Jazeera 2018; Head 2017; Myanmar Now 2019).

As with Hitler's Secrecy Order, the legislation under which Lone and Soe were charged – the colonial-era Official Secrets Act – contains no limits for government secrecy and does not prohibit using secrecy to conceal crimes. Nor does the Official Secrets Act exempt individuals who disclose "state secrets" that prove state involvement in crimes. On the contrary, the only factual element required to sustain a criminal prosecution is that the accused "retain[ed] any official document, whether or not completed or issued for use, when he has no right to retain it" (AsianLii 1923). Accordingly, in September 2018, the journalists were convicted and sentenced to seven years in prison (PEN America 2019). The decision was later upheld by the Yangon Region High Court in January 2019 and again by Myanmar's Supreme Court in April 2019 – which determined that the journalists had intended harm for the country via their publications (PEN America 2019; Naing and Lewis 2019).

Russia

In Vladimir Putin's Russia, the methods employed to conceal state crimes are somewhat more nuanced than in other closed systems. On the one hand, as is the authoritarian norm, Russian intelligence agencies like the Federal Security Service (FSB) retain a near-total right to sequester all internal departmental information. In exercising this right, the FSB has exceptionally broad latitude to not only decide what is and is not a state secret but also to preventatively police "conditions" that impede upon the state's interests (BBC 2012), including through aggressive censorship (Roskomsvoboda 2018). Of note in Russia's FSB Law, information blanketed by a secrecy privilege includes all information about "[FSB] servicemen" and any information "on the organization, tactics, methods and means deployed by [FSB] organs…in carrying out operational activities" (Russian Federation 1995; 2012). There is no identifiable exception to the FSB's default right to secrecy. Under this law, an FSB officer cannot legally be identified as a participant in "operational activities" even if those activities were to constitute an international crime.

Despite this comprehensive "closedness", the Russian Federation still maintains some institutional facets which purport to be imitatively "open" – a vestige of the *glasnost* years which precipitated the Soviet Union's collapse. One such "openness" fig-leaf is a never-enforced rule in Russia's On State Secrets law which explicitly directs that information "about violations of laws by organs of state power and their officers" is "intelligence [that is] not subject to be referred to [as] state secret and classified" (Russian Federation 1995; 2012). Consequently,

according to the law On State Secrets (but not according to the FSB Law) Russian intelligence activities that constitute criminal offences cannot be state secrets.

To skirt around these legal contradictions, the ex-KGB strongmen who have controlled Russia since the end of the Cold War, have employed a mixed-methods approach when targeting civil society actors who expose state-orchestrated atrocity crimes. Commonly employed methods include punishment through *indirect legal* avenues (in contrast to the *direct* prosecutorial approach in Myanmar) and extrajudicial killings carried out by an element of the Russian intelligence community.

When legal avenues are pursued, one Russian government tactic is to recategorize whistleblower disclosures as something other than disclosure about atrocity crimes – for example, by alleging that the information is false and damaging to Russian social cohesion. This was most recently seen in the criminal cases against the journalists Pyotr Verzilov and Ilya Krasilshchik, who covered the Russian military's 2022 massacre of Ukrainian civilians in Bucha (Committee to Protect Journalists 2023, Meduza 2023). In the Verzilov case, charges related to four Instagram and Twitter posts in which he described the massacre as "one of the monstrous crimes of the 21st century" (Verzilov 2022a); reported on the execution of an old man "at point-blank range" (Verzilov 2022b); captured video at a mass grave (Verzilov 2022c); and characterized the perpetrators of the killings as "Hitlerite and Stalinist bloody scum" (Verzilov 2022d). According to the prosecution's filings, Verzilov's reportage did not evidence mass murder (although, of course, it *did*) but instead "created a real threat of forming a false opinion among citizens about the goals and objectives of the special military operation" (Mediazona 2023). In the Krasilschchik case, the former publisher of the investigative news website *Meduza* was similarly charged for his Bucha reporting – accused of "spreading fakes" (Meduza 2023).

In other cases, Russian prosecutors lay retaliatory charges that are completely unrelated to the actual whistleblowing, even if the disclosure is the true motivation. In the case of Aleksey Navalny, whose work as an anti-corruption activist saw him report on an FSB attempt to murder him with a Novichok nerve agent, "sham" charges included theft of lumber (Amnesty International 2022a) and contempt of court (Amnesty International 2022b). Under the FSB Law, the Russian government presumably had domestic avenues to pursue Navalny for publishing the names of FSB officers who had poisoned him. However, those charges were never laid. The aim, one might infer, was to suppress Navalny's coverage of the poisoning, drawing the Russian public's attention away from it.

In another case involving a combination of direct and indirect charges, the lawyer Mikhail Trepashkin (a former FSB officer himself), was jailed for illegally possessing a firearm and for divulging unspecified "state secrets" (Rodriguez

2004).[16] Trepashkin had previously fallen afoul of the FSB bureaucracy, having written to President Yeltsin alleging that organized crime groups had penetrated the service (Anderson 2017). But the final trigger for Trepashkin's arrest was a public announcement that he had uncovered evidence of FSB involvement in the 1999 Russian apartment bombings – a spree of terrorist attacks which Putin had leveraged as a pretext for war in Chechnya. Of note, Trepashkin claimed to have discovered that a basement space used by the bombers was in fact rented by an FSB officer (Rodriguez 2004). Trepashkin was convicted and sentenced to four years in prison (Murphy 2004). This judicial outcome both removed Trepashkin from the field of potential whistleblowers and effectively ended the investigations of a Russian parliamentary commission that was examining the bombings (Commission on Security and Cooperation in Europe 2004).

Outside legal processes, Putin's FSB also uses *extra*-legal means to deal with whistleblowers disclosing state crimes. Here, the preferred approach is usually violence. As a tool with a *longue durée* in Russian political history, assassination methods have changed over time – ranging from gun murder at close range to the deployment of chemical or radiological weapons.

One high-profile assassination that was clearly responsive to atrocity whistleblowing was the murder of former FSB officer Aleksandr Litvinenko. A veteran of the FSB's counter-intelligence service (where he specialized in counterterrorism and organized crime), Litvinenko's post-government career saw him author two books alleging criminal activities inside the FSB. The second of these books, *Blowing up Russia: Terror from Within* (Felshtinsky and Litvinenko 2002) furnished new incriminating details about alleged FSB involvement in the 1999 apartment bombings. The book also claimed that the 2002 Moscow theatre hostage crisis was provoked by an FSB informant.

Prominent in *Blowing up Russia* was a focus on a failed FSB attempt to place explosives in a Ryazan apartment building, an enormously controversial episode which framed larger narratives about state complicity in the bombings (Felshtinsky and Litvinenko 2002). According to security forces officials quoted by Litvinenko, initial testing of the Ryazan devices indicated that "fumes of a hexogen-type explosive substance" were present (Felshtinsky and Litvinenko 2002: 64). As one militia officer put it: "no one had any doubt that this was a genuine emergency situation" (Felshtinsky and Litvinenko 2002: 63). This forensic evidence contradicted the FSB counter-narrative, whose then-Director Nikolai Patrushev would later claim that the bombs were dummy devices; that they were positioned as part of a counter-terrorism exercise; and that they contained sugar, not explosives (CNN 1999). Despite these claims, Litvinenko noted that they were contradicted by the Ministry of Internal Affairs (MVD) and the municipal authorities' own lack of awareness of the existence of a counter-terrorism exercise (Felshtinsky and Litvinenko 2002: 70–71).

In response to this damning material, the Russian government banned *Blowing Up Russia* for divulging "state secrets", adding it to Russia's "Federal List of Extremist Materials" (Prima News 2004). Four years later, in an operation assessed to have been ordered by Putin himself (Owen 2016: 244), the FSB assassinated Litvinenko with polonium-210, a highly radioactive, gamma ray-producing polonium isotope.

In other suspected assassinations of atrocity whistleblowers, killings appear to have been carried out in a less spectacular, plausibly deniable manner. A noteworthy example is the eventual death of Aleksey Navalny in an Arctic prison – officially a suspicious "death in custody" but characterized by the United Nations (2024) as the culminating event of an "enforced disappearance".

Another example is the 2006 contract killing of the journalist Anna Politkovskaya. While Politkovskaya's murder was never definitively attributed to the state, her killing is widely believed to have been retaliation for her journalistic work – namely, her reporting on torture in Kadyrov's Chechnya (Bigg 2006); her investigation into an alleged mass poisoning of Chechen school children (Politkovskaya 2006); and her trenchant criticisms of Putin and the FSB (Politkovskaya 2004). State attribution was further indicated when it was revealed that the FSB had hacked into Politovskaya's email account before she was murdered (Biddle 2016), substantiating concerns that her movements were being tracked at time of her death.

As these cases collectively illustrate, the operationalization of criminal secrecy in Putin's Russia is somewhat *sui generis*. In its capriciousness and its internal contradictions (i.e., the written rules for secrecy are often not the *actual* secrecy rules), the sense is that the system runs on a case-by-case basis. It is situational rather than structural authoritarianism. While it ostensibly remains illegal to bury atrocities using secrecy in Russia, the history of concealment and punitive retaliation clearly connects the Putin regime to other closed, authoritarian systems.

In all these closed systems, the consequences for international justice are the same: state perpetrators continue offending; whistleblowers are deterred from making disclosures; and any attempts at genuine accountability are structurally frustrated, by default.

Criminal Secrecy in Open Societies

In contrast to closed societies, where states conceptualize secrecy obligations in absolute terms (with no exceptions, even for atrocity disclosures), open societies are defined by a formal balancing between the government's right to safeguard information and the right of individual citizens to know about it. Open societies push back against the underlying premise of the "reason of state", rejecting the view that rulers may act in ways that contradict natural law. In principle and in

practice, this rejection of unlimited executive power acts to constrain public officials, protecting against the proliferation of criminality in government. These constraints are underwritten by a constitutional separation of powers and the Damoclean presence of an independent judiciary. Although, as we shall see, these checks and balances are often ineffective, the existence of formal and informal "guardrails" is nevertheless a feature of open governments (Tushnet and Bugaric 2022).

Connected to these "guardrails" and tied to the liberal conception of "openness" is the principle of transparency – which works to make the decisions of government accessible so that they can be scrutinized and, where required, criticized (Government of Canada 2024, Worthy 2017).[17] While the chosen amount of transparency is always weighed against privacy and "national security" considerations, the transparency principle still informs how open bureaucracies manage the keeping of official secrets.

Accordingly, there is, at the very least, formal consensus within open governments that the purpose and justification for secrecy is not to conceal wrongdoing by the state – least of all *criminal* wrongdoing. "Over-classification" is also regarded as a procedural problem, even if done for innocent reasons, because it hampers the flow of operationally important information, preventing it from reaching necessary destinations (NZ Protective Security 2025).

Because open governments are thus restricted by systems of *limited secrecy*, a much sparser range of tools is available to state actors trying to conceal atrocities. Available tools include unofficial secret-keeping processes (*informal secrecy codes*); the abuse of the classification system (*motivated over-classification*); and the misapplication of "protected identity" policies to conceal guilty party attribution (*perpetrator anonymization*). Lacking the full range of legal and extra-legal tools that totalitarian governments enjoy, open governments also have fewer means to punish whistleblowers.

Using case studies from states within the "Five Eyes" (FVEY) multi-national intelligence alliance, a comparative history of abusive secrecy in open societies is described below.

The "Five Eyes" Alliance

To understand how open government bureaucracies set limits on secrecy, it is worth examining relevant laws and policies within the Five Eyes (FVEY) intelligence alliance – which comprises the USA,[18] Canada, the UK, Australia, and New Zealand. By design, the principles articulated in FVEY information security policies are nearly identical because a cornerstone of the alliance is a common information-sharing framework that stresses the importance of safeguarding "national security*"* information in ways which still comports with shared democratic values.

In the USA, the limits of secrecy are tied to criminal activity – as seen in Presidential Executive Order 13526, which prohibits placing security classification markings on information to "conceal violations of law, inefficiency or administrative error" (US National Archive 2009).

In Australia, the Protective Security Policy Framework (PSPF) similarly states that "it is not consistent with this policy to apply a security classification to…hide violations of law, inefficiency, or administrative error or to prevent embarrassment to an individual, organization or entity" (PSPF 2023). On the specific issue of Australian war crimes, Assistant Inspector-General of the ADF Major-General Paul Brereton remarked further on these limits when he observed that "no obligation of secrecy attends criminal conduct, even if it occurs in an operational setting" (Inspector General of the Australian Defence Force 2020a: 114, 326).

In New Zealand, the Information Security Classification System Policy states that a document's originator must not use classification markings to "hide violations of law, inefficiency, or administrative error". The New Zealand policy also prohibits applying a security caveat to "prevent or delay the release of information that does not need protection in the public interest" (NZ Protective Security 2022).

In Canada, relevant information security policies state that the classification system must not be used to classify information that is unrelated to "the national interest" (Treasury Board Secretariat 2019) and that "information is not to be safeguarded…to conceal inefficiency, errors or problems" (National Defence 2022).

Last among the FVEY allies is the United Kingdom. Although the UK Ministry of Defence's (MOD) classification policy does not explicitly prohibit using security markings to hide criminality, the MOD's joint intelligence doctrine warns that "over-classification" is a significant operational impediment because it "causes delays in [the] handling and transmission" of mission-critical information (UK Ministry of Defence 2023: 69). Implicitly, such "delays" include delays to the exercise of law enforcement functions.

That UK law contains no basis for concealing atrocity crimes with official secrecy was further clarified during the UK's Independent Inquiry relating to Afghanistan (IIA), evidenced in a high-profile exchange between inquiry senior counsel Oliver Glasgow KC and Johnny Mercer, the UK's then-Minister of State for Veterans' Affairs (Independent Inquiry relating to Afghanistan 2024).

Johnny Mercer:	You've got to understand Mr Glasgow, to speak about these [special] operations outside of that environment is breaking the law…is breaking the Official Secrets Act…
Oliver Glasgow KC:	You are wrong Mr Mercer when you say that. It may very well be a genuinely held belief by you but before you suggest that people should be concerned about coming

> forward [about war crimes] because of the Official Secrets Act…no one should think as a result of what you've just said that they can't come forward because they might be breaking the law.

Resultingly, there is agreement across the FVEY alliance that the unchecked and inappropriate use of secrecy is an obstructer to the good business of government (especially law enforcement operations) as well as the transparency aims of an open society. It thus follows that just as there are obligations to sequester information that will cause harm if disclosed, the FVEY information security framework carries a flip-side obligation *not* to compartmentalize or conceal information unnecessarily. Information that would implicate oneself or one's organization in criminal wrongdoing is information that would self-evidently *not* be security classified under these policies' basic principles.

Nevertheless, abusive secrecy practices still exist in these governments – including in relation to atrocity crimes. The three most common methods for achieving this (*informal secrecy codes*, *motivated overclassification*, and *perpetrator anonymization*) are discussed below.

Informal Secrecy Codes

Beset by a regulatory framework that prohibits using secrecy to cover-up crimes, one way that officials in open societies hide such information is through *informal secrecy codes*. A case-in-point is seen in the abusive secret-keeping within Australia's Special Air Service Regiment (SASR) during the War in Afghanistan. In his analysis of a years-long pattern of war crimes by the SASR, Major-General Brereton was highly critical of "a culture of secrecy and compartmentalisation" within the unit. Brereton was especially critical of secrecy practices among non-commissioned officers where "loyalty to one's mates, immediate superiors and the unit [we]re regarded as paramount" (Inspector General of the Australian Defence Force 2020a: 37). According to Brereton, the SASR's generalized culture of secrecy gave rise to a more specific "code of silence" (Inspector General of the Australian Defence Force 2020a: 29) at the patrol level. In practice, this "code" unambiguously sequestered incriminating information within the selected "operator" in- group, deterring the disclosure of peer atrocities (IGADF 2020a: 37). The "code" had explicit caste- based character-istics (in which elite "operators" were socially differentiated from "supporters"), as pithily described by one of the operators themselves, in leaked helmet camera footage. As the soldier stated in his criticisms of another soldier's exhibitionist crimes: "[He] execute[d] someone in front of support staff… You can't do it in front of anyone but a fuckin' operator" (ABC 2020).

Years later, as information about the SASR's war crimes began to bubble to the surface (often because of "support staff" whistleblowing) one of the more notorious perpetrators, Victoria Cross recipient Corporal Ben Roberts-Smith, was recorded on tape imploring a trial witness to "stick to the code" (*Sydney Morning Herald* 2023).[19]

The importance of this "code" within the SASR necessarily raises questions about how a soldier might be initiated into such a secrecy custom. While the Army's SASR training pipeline provides a partial explanation ("unconventional" operators are specially "selected" from the "conventional" forces), more specific initiations into criminality are seen in practices like "blooding" – a gang-like rite in which new operators were coerced to murder a prisoner as their "first kill". Sociologically, "blooding" has a similar function to the Sicilian Mafia's "earning one's button" custom. Another analogue is the secretive *sicario* inductions within Mexican cartels, where initiation practices involving cannibalism have been reported (Pope 2024). In all these examples, participation in the in-group secret – namely, the deep secrets of the criminal conspiracy – depends on first joining the enterprise by committing a murder and implicating oneself.

Because these secrecy practices are predicated on tiered membership and progressive initiation, the SASR's "code"-based concealment system also replicates similar patterns in some religious sects, where care is taken to incrementally introduce new initiates to forbidden arcana. As Simmel notes of newcomer assimilation into such groups: "graduated secrecy produces at the same time an elastic zone of defense for that which is inmost and essential" (Simmel 1906: 488), providing mutual assurance and lending form to the union itself. Incrementalist admittance thus performs two functions at once. It is, simultaneously, a protectant against unexpected reactions from the initiate while they are being initiated *and* a basis for further compounding the group's sense of togetherness. In the case of "blooding", the continuing existence of the joint criminal enterprise within the SASR depended on the secrets of the initiation remaining so.

Motivated Over-Classification

In the interests of fairly characterizing the mechanics of abusive secrecy within Australia's special forces, it needs to be stressed that concealment was not endemic to junior soldiers at the patrol level *only*. Indeed, even though soldiers in lower-level formations possessed their own microsocial norms (blooding was only a systemic practice in the SASR's 2nd Squadron), a large body of evidence from across FVEY special operations units suggests that secrecy practices were also abused at the higher level, often to the same effective end. Rather than a small-team aberration concocted *ex nihilo* by the rank-and-file, operator "compartmentalization" was merely a local manifestation of a much wider policy that unpleasant

information, as a general rule, ought not to be disclosed. One way this manifested is in the misuse of the security classification system to stymy the flow of incriminating information.

The practice of *motivated over-classification* was particularly rife in UK Special Forces (UKSF) units in Afghanistan. An egregious example is the decision of General Gwyn Jenkins, a then-UKSF unit commander, to authorize the creation of a tailor-made information security compartment whose sole purpose was to conceal allegations of extra-judicial killings (acronymized as "EJK") (BBC 2023). As the document rather banally reads:

> As directed by CO…a Security Compartment will be generated in order to protect information pertaining to the possible involvement of [REDACTED] in EJK. The Compartment Owner will maintain all 'Master' Compartment documentation. The [Focal Point Officer] will be responsible for the local reading on of relevant SFHQ(UK) personnel (Independent Inquiry relating to Afghanistan 2025).

Within Jenkins' Security Compartment, the "Disclosure Level" for each access-permitted officer was further broken down into four sub-compartments. The broadbrush "Detail of Allegations" was listed as Level 1 and "Full Disclosure" (which included perpetrator identities) was listed as Level 4. Only five UKSF officers were "read-in" to this compartment, with military police completely excluded from the Access List.

Less brazen but much more pervasive was the presence of the "UK Eyes Only" (UKEO) security marking on numerous documents implicating UKSF members in other war crimes. As with the security markings on Hitler's Commando Order, the "UKEO" security markings on these documents explicitly directed recipients *not* to convey the information outside a clearly defined circle of knowledge – in this case, any non-British citizen. The practical effect of this ensured that the American International Security Assistance Force (ISAF) Commander did not receive the "EJK" allegations, even though he had operational responsibility for British troops on the ground.

National "Eyes Only" siloing of incriminating information was also happening concurrently within the Australian special forces. For example, in the aftermath of a 2012 alleged double war crime in the Afghan village of Sola, ADF officers attached an "Australian Eyes Only" (AUSTEO) caveat to an inquiry report about the incident (ABC 2017). Again, the effect of this caveat was to impede the onward transmission of incriminating information to the American ISAF Commander. A further "communications pack" was also appended to this AUSTEO report, recommending that the information not be made public following a "consideration of Australia's national interest".[20]

Other evidence indicates that report-siloing was happening at even higher levels within the ADF. This is mostly clearly demonstrated in then-CDF General David Hurley's August 2014 order that he alone was the "sole delegate" for disclosing inquiry reports (Defence Australia 2023). Whether intended or not, the logical takeaway for any soldier who might have read this order was that General Hurley was prohibiting the disclosure not only of the reports themselves but also the evidence of possible crimes that contained within them. As with the UKEO and AUSTEO security caveats, the practical effect of the order was to impede the flow of information to the American general commanding ISAF.

Motivated overclassification continues to blight the Australian government's reckoning with these crimes, even years later. This was seen as recently as 2020, when ADF officers issued orders not to disclose war crimes-related information to anyone outside the Defence Department. During these "Records of Conversation", one soldier witness to a war crime was directly warned by his squadron sergeant-major that disclosing "official information" to "any third party" could be grounds for criminal sanctions (Special Broadcasting Service 2023).[21]

It is difficult to precisely assess what impact these "Conversations" had on individual soldier disclosures. Glenn Kolomeitz, a former legal officer in Australia's special forces, has observed that ordering a soldier not to disclose such information to "third part[ies]" outside the Department of Defence could reasonably be interpreted as an order not to disclose such information to the *police* (Special Broadcasting Services 2023). Either way, it is open to infer that these warnings had at least *some* deterring impact on the passage of information.

A second illustration of directed non-disclosure was seen in a "Communication Plan" and "Security Directive" issued by ADF in the build-up to the release of the Brereton Report. These documents warned special forces soldiers that only the CDF was authorized to speak publicly about Afghanistan Inquiry matters and that the appropriate response to journalistic contact was to "take a screenshot of the message(s) before blocking the contact". A carefully worded script was also provided should any special forces soldiers be approached face-to-face (Defence Australia 2025b).

Beyond the rank-and-file, Australian lawyers acting for the Commonwealth also seem to have used "national security" logic to deter others from disclosing war crimes-related information. The experience of Samantha Crompvoets, the sociologist whose research into the culture of Australia's special forces triggered the Brereton Inquiry, provides a near-perfect demonstration of this. As Crompvoets recounted to ABC News:

> I was threatened by the Australian Government Solicitor after I had published my book [about Australian war crimes]. They said I had done harm to the

> Commonwealth and therefore the Commonwealth had lost trust in me… my contracts were cancelled with Defence… (ABC 2023)

In all these cases, the substantive effect of the secrecy practice (whether formal or informal) was the same. Whistleblowers were deterred from reporting what they knew (either through the mere suggestion of punishment or by incurring actual losses to livelihood) and information remained hidden.

Perpetrator Anonymization

A third way that open governments skirt prohibitions against concealing atrocity crimes is by tailoring the suppression to the perpetrators' identities. Because an identity necessarily involves personal information, the state will co-characterize personally identifying information as privacy-related information *and* "national security" information. Concealing atrocity attribution via abusive "protected identity" provisions is relatively widespread in open democracies – especially when atrocity perpetrators have ties to intelligence or special operations organizations (whose activities are, often justifiably, sensitive).

The classic case is CIA officer John Kiriakou's conviction for disclosing the names of intelligence officers involved in the CIA's post-9/11 torture programme (Schmidt 2013). Although Kiriakou's disclosure arguably advanced the interests of justice (the revealed names were subsequently inserted into another proceedings as part of defence submissions), the US government nevertheless prosecuted the conduct under the Intelligence Identities Protection Act. At Kiriakou's sentencing hearing, the judge asserted that "this is not a case of a whistleblower…you have already spoken too much" (Schmidt 2013).

In Australia, similar laws exist to conceal the identities of intelligence officers, but they do not extend to the special forces (least of all *former* members of the special forces implicated in war crimes). Despite this, the ADF touts its own internal policy that grants so-called "protected identity status" (PIS) to special forces personnel. This pseudo-protection against public identification is not enforceable outside the ADF chain-of-command and carries no special privileges in legal proceedings "beyond those protections available to all Australian citizens" (Defence Australia 2025a).

Lacking a statutory basis, PIS is also a fleeting privilege, being fixed to specific duties and responsibilities. As Chief of Defence Force (CDF) General Angus Campbell described the policy's coverage: "protected identity status is active only while those persons are undertaking [special operations] duties…. It is not active when they no longer serve in the Australian Defence Force" (Commonwealth of Australia 2023: 18).

Despite the policy's very limited internal protections, at various times the Australian Special Operations Command (SOCOMD) has lobbied to transform

PIS into a legally enforceable protection, comparable to that enjoyed by intelligence officers. Special forces veteran groups have also lobbied for more identity protection, as seen in 2nd Commando Regiment officer Heston Russell's parliamentary petition to suppress the identities of accused war criminals during trial (Veteran Support Force 2023, Parliament of Australia 2023).[22]

From the perspective of legislative review bodies, this lobbying has largely landed on deaf ears. As former Director-General of Security Dennis Richardson observed in his review of Australia's protected identities framework: "The Review does not consider there is a need for a specific secrecy offence to protect SOCOMD identities…the degree of harm arising from the disclosure of the identity of SOCOMD personnel is substantially lower than that of [intelligence] officers" (Richardson 2019). Richardson's reasoning did not only rest on the different mission sets (e.g., the fact that disclosing an intelligence officer's identity may collaterally threaten the life of a human source). Richardson also noted that former SOCOMD personnel often self-disclose their professional experiences in popular media, disproving the notion that lifelong anonymity is founded in a genuine security concern.

In spite of Richardson's clear-eyed observation that special forces identities do not constitute "national security" information, Australian government departments have often misstated this fact, including in court proceedings. A near-perfect illustration was in *Roberts-Smith v Fairfax*, a defamation case which examined whether Ben Roberts-Smith committed a series of war crimes reported by Fairfax Media. During the proceedings, two separate Australian government departments led the presiding judge to believe that any "information identifying Special Forces" personnel was "operationally sensitive and/or security classified" (Inspector General of the Australian Defence Force2020b: 8) such that every "current or former member, officer or employee" associated with SOCOMD ought to be considered a "sensitive witness" subject to anonymization under a *National Security Information Act* suppression order (Australian Government Solicitor 2020).[23]

In making these arguments, there was a palpable discrepancy between the effort to suppress the names of Australian war crimes suspects and the apparent lack of protections for Afghan witnesses remotely testifying at trial. All the Afghans were publicly named during the proceedings, despite being physically located in Taliban-controlled Afghanistan (Federal Court of Australia 2022a).[24] After accepting the government's arguments that identity protections were required, the presiding judge approved the suppression request, thus transforming PIS from a secrecy practice that had no basis in law into one that did.

The anonymity affordances were promptly abused. As the proceedings unfolded, Roberts-Smith-aligned SASR soldiers took to Instagram to excoriate lawyers acting for the media. Afghan victims were labelled "terrorist p3dos" and

soldiers who had helped the media expose the crimes were castigated and doxed, accused of being "rats" who were "dogging the boys" (Doherty 2022b; McKenzie 2023; McHugh 2025). At least one of the SASR soldiers amplifying this material was an identity-protected witness in the proceedings (Doherty 2022a).

As the online conduct continued, actors located outside of Australia used the Instagram activity (and accompanying information on the court's YouTube channel) to identify Roberts-Smith-aligned witnesses online. This drew a livid response from Roberts-Smith's lawyers. But as the judge presiding would later observe, there was no way to prevent such publications since they were occurring beyond the court's jurisdiction (Rimington 2022, Federal Court of Australia 2022b).[25]

As with anonymity crimes committed by other criminal groups,[26] the Roberts-Smith camp's online activity was not endorsed by the Australian government *per se*. The government simply provided an affordance for the conduct by creating a state of exception (an identity protection schema that had no precedent) that perpetrators then exploited.

The online vilification of soldiers working against Roberts-Smith also provides a tidy illustration of *punishment by perpetrators* – an all-too-common outcome for whistleblowers who are otherwise unlikely to face direct legal punishment from the state.

International Justice Outcomes

Besides emboldening perpetrators to act with impunity, secrecy can also frustrate legal proceedings, preventing the proper punishment of crimes. In a 2001 case related to alleged Australian SASR war crimes in East Timor, proceedings collapsed because New Zealand refused to allow its soldiers to testify, fearing the disclosure of special forces identities in open court (Snow 2003). In an analogous domestic criminal case, a Canadian JTF-2 soldier was accused of assaulting a subordinate. Despite the seriousness of the offence, the judge dismissed the case because, as *The Star* put it, "the unit is protected by such secrecy that none of its members can be named" (Maccharles 2006).

Naked political interference is another problem when "national security" is invoked in atrocity crimes cases. During an Australian Senate Inquiry examining the requirement that the Attorney-General personally consent to genocide prosecutions, the government submitted that "international relations" and "national security" were among the factors that determine whether a case should proceed (Attorney General's Department 2024: 4). As one senator portrayed this approach: "it might negatively impact on our relations with a friend…and for that reason we wouldn't prosecute a perpetrator of genocide" (Commonwealth of Australia 2024: 45).[27]

Beyond domestic contexts, the (mis)invocation of "national security" – whether by a closed or open government – seems likely to frustrate international court processes in the future. There were hints of this in the Roberts-Smith trial[28] but it is also overt in the laws of some Rome Statute signatories, where "national security" exceptions are inked in as an escape hatch to avoid certain forms of cooperation (International Criminal Court Act [UK] 2001, sec 39; International Criminal Court Act [Aus] 2002, sec 145–149).

An even trickier problem for international justice relates to whistleblower protections. Whistleblowers with insider knowledge are naturally of great interest to war crimes investigators, whether domestic or international. But they are disincentivized to report what they have witnessed for many reasons. Within military organizations, reasons for soldier non-disclosure include direct peer pressure; feelings of unit loyalty; the brotherly "all-for-one" bonds that are unique to soldiering (where in-group fealty amounts to "fictive kinship"); and the practical desire to not impede the output of an otherwise non-odious military operation. By themselves, these pressures already create crippling uncertainty for soldiers. To then work one's way through conflicting duties (the duty to disclose and the duty to uphold secrecy obligations) further increases that dilemma.

This was perfectly encapsulated in one US Army interrogator's belief that he could not report the abuse of Iraqi prisoners because he would be breaching the non-disclosure agreement he signed with the special operations task force employing him. As the interrogator later recounted to Human Rights Watch:

> We didn't have CID there [the US Army's Criminal Investigative Command]…. Camp Nama was completely closed off…[reporting to CID] was problematic. I mean are we violating our NDA?…Because they had this special order…from the Pentagon…they supercede any other. You can't even tell your chain of command (Human Rights Watch 2006)

As this case shows, concerns about law-breaking clearly deter soldiers who would otherwise have no moral objection to reporting atrocities. These concerns are nested in fears of punishment, rather than a philosophical affection for keeping crimes a secret.

Indeed, for whistleblowers everywhere, there is proof aplenty that governments (both open and closed) will go to massive lengths (both legal and extra-legal) to deter secrecy breaches. The $2.6 million prosecution of David McBride (Shoebridge 2025) and Alexander Litvinenko's technically convoluted assassination with polonium are just two cases to draw on here.

The history also shows that a whistleblower's station or status is unlikely to be an effective shield against executive action. In a recent case, the IDF's Military

Advocate General was arrested for disclosing video evidence of prisoner rape at the Sde Teiman detention facility (Graham-Harrison 2025), demonstrating that whistleblower punishment will always be a default priority, regardless of rank.

The case of Milan Levar, a Croatian Army reconnaissance commander who was murdered after submitting evidence to the International Criminal Tribunal for Yugoslavia (ICTY), raises additional questions about the capacity of international courts to protect witnesses across borders, even when states are notified of their status and relationship with international prosecutors. After Levar publicly accused the Croatian Army of war crimes, the ICTY Prosecutor wrote to the Croatian government requesting witness protection measures (International Criminal Tribunal for Yugoslavia 2000). Despite agreeing to do so, the Croatian government never passed these instructions to the local police in Gospić. Gospić was not only the town where Levar lived – it was also the place he had witnessed the massacre of Serb civilians (Hedges 1998). Levar was killed in a car bombing on the driveway of his mother's Gospić home (Smith 2000).

Together, these cases suggest one conclusion: whistleblowers can expect to encounter serious dangers on the pathway to disclosure. The result is a severe impact on international justice outcomes. Without more serious efforts to resolve this problem, the concern these impediments raise is that atrocity whistleblowing may be diametrically opposed to secrecy structures *in general*.

Pathways for Addressing Criminal State Secrecy

In 1945, while working as a prosecutor in the largest murder trial of all time, Benjamin Ferencz cracked open an archive of "Top Secret" Nazi files. In fastidious detail, the documents outlined the Holocaust's inner workings (Ferencz 1999). Without these documents, it is possible that the Einsatzgruppen prosecutions at Nuremberg would not have occurred. What are we to make of this? One conclusion is that Ferencz's *main* adversary was not the Nazi genocidaires themselves nor the arguments their lawyers would use to litigate the discovered "Top Secret" facts. Rather, Ferencz's real nemesis was the secrecy which had isolated these facts from his investigators until the archive's discovery, by accident.

This exemplifies a more general problem that totalitarian systems pose for international justice. As closed systems conceive it, the tension between "national security" and "international security" is not actually a tension because, as Bergson notes, "[its] members hold together, caring nothing for the rest of humanity, on the alert for attack… bound, in fact, to a perpetual readiness for battle" (cited in Hammersley 2024: 1423) Totalitarians also assert a right to act in ways that are not only inhumane, but are actively *anti*-humane – as indeed, the Holocaust illustrates. In this way, the Nazi concept of "national security" was *inherently* a threat to international security.

In the context of democracy, Ellian and Cliteur argue that closed communities within open societies may pose their own threat to liberal orders (Elian and Cliteur 2021). While, in open government bureaucracies, there is no "duty to conceal" atrocities as such, the possibility remains that atrocity-concealing communities will still form among "the many princes of our secretive republics" (Sagar 2013: 204).

The security classification system is the easiest secrecy tool to abuse here, for a very simple reason. Not unlike a water faucet, the caveats appended to government information determine the volume of its flow and the number of its recipients. When the faucet remains closed or its contents are too sparingly decanted, security caveats can become obstructive. This is well-evidenced in the FVEY cases discussed in this study.

Bemoaning the transformation of a "legitimate system of restriction" into "an extravagant and indefensible system of denial", Arthur Schlesinger, a former intelligence analyst and court historian to President Kennedy, was an early critic of abusive secrecy (cited in Sagar 2013: 16). Seemingly though, this problem was never as bad as it was in Afghanistan, where motivated overclassification was explicitly used to hide crimes. The conflation between what could rightly be called "international justice" information and "national security" information is perhaps best encapsulated by one NZSAS officer's response to reports that troops under his watch had killed civilians: "as you know there is a very real security threat that could result if the Kiwis are in any way linked to the Burnham job" (Burnham Inquiry 2020).

This does not mean that genuine national security interests never attach to atrocity-related information. What is obvious though is the absence of balance. If it is true that atrocity crimes threaten the security interests of all mankind, then concealing their commission necessarily broaches on supranational, species-level concerns.

How, then, do we resolve this foundational tension? There is no dispute that improperly disclosing secrets can compromise panoply government equities, with potentially catastrophic consequences. Nevertheless, states must work harder to correctly distinguish between genuine vectors of harm and the spurious, imaginary harms that are often conjured when "national security" is invoked. Open governments already have policies to conduct such injury tests, but the foregoing history suggests that this is insufficient.

Moving forward, states should more plainly state – in policy and in statute – that information incriminating the government in war crimes, crimes against humanity and genocide are not to be considered "state secrets", *as such*. One technocratic solution could involve labelling atrocity-related material with an "INTERNATIONAL LEGAL" caveat, rather than a "SECRET" one – that is, by

mandatorily placing such information in its own category. Beyond sharpening the distinction between these information types, marking documents in this way would also signal that such material ought to be disclosed to a competent criminal investigator or, indeed, an officer of the International Criminal Court. This could help prevent the recurrence of abusive compartmentation in the future. Absent significant change, the status quo operationalization of secrecy will eventually undermine the integrity of these classification systems as a whole.

Strengthening the effectiveness of internal and external channels for atrocity whistleblowing is another area in need of improvement. While whistleblower channels are notionally present in open governments, their effectiveness is highly debatable. As the McBride case shows, it remains incredibly risky to bring atrocity-related information into the public domain, even in the so-called liberal democracies.

Given the scope and complexity of the problem that abusive secrecy poses, an international treaty may eventually be required to resolve all related issues. And assuming that individual state actors cannot be *automatically* trusted to responsibly balance the tension between national security and international justice, it is perhaps time to collectively outlaw the methods of atrocity concealment described. Without serious, concerted intervention, the problem will endure.

Notes

1. 207 of the 235 documents were marked "SECRET". Some were also marked with a highly specific "Australian Eyes Only" (AUSTEO) dissemination control (*R v McBride*; ABC 2017).
2. McBride's sentence attracted special interest because it occurred amid increasing public concerns about government corruption and prosecutions of other whistleblowers who had disclosed illegal activity by the Australian government (Human Rights Law Centre 2025, Zifcak 2020).
3. The three types of atrocity crimes are war crimes, crimes against humanity, and genocide.
4. This article will alternately refer to "criminal secrecy" as "abusive secrecy".
5. As Plato writes of the god Uranus' castration by Cronos "even if [the myth] were true [it] ought certainly not be lightly told to young and thoughtless persons" lest they follow in the suit of "the first and greatest among the gods" (Plato 1991: 73)
6. Clapmarius developed his *arcana imperii* concept from Tacitus' terminology for the secrets that underwrote the power of the Roman emperors.
7. Clapmarius qualifies his endorsement of the "right to dominate" by asserting that laws should not be violated thoughtlessly because the ruler "should not use his power where laws can be acted upon" (Clapmarius 1644" 23–24).
8. The Italian philosopher Giorgio Agamben traces a genealogy between the Nazi regime's "willed state of exception" (*geowollte Ausnahmezustand*) and Gratian's narrower proposition that a violation of law may be excused by specific, circumscribed necessity (*necessitas legem non habet*) (Agamben 2005: 3, 24–26)
9. In one infamous retaliation, the son of a Mafia *pentito* was kidnapped, strangled and dissolved in nitric acid after his father provided information to Italian prosecutors. A note was sent to the father reminding him that *omertà* inductees "shut our mouths" (Corriere 2010).

10. Beamish's examination of cultures of silence in the petroleum industry identified that "pressure to keep the spill a secret, based in a de facto culture of silence" (Beamish 2000: 486) is found across the whole workforce and often led down some extraordinarily dark paths.
11. Although helpful for model simplification, the use of a binary typology necessarily raises an analytical problem regarding tough cases – for example, when a society is transitioning from a system of limited secrecy to a more totalitarian one. In Israel, for example, Israeli-owned media organizations are legally able to disseminate information about Israel Defense Force (IDF) crimes while Arabic media organizations, such as Al-Jazeera, now face reprisals for doing the same (Amnesty International 2024, Usher 2025). This suggests that Israel's relative "openness" is contingent, transient and potentially dwindling. In freely acknowledging that such tough cases do exist (indeed the behaviour of many so-called "liberal democracies", is often much less "open" than their leaders claim), the issue is considered a methodological limitation, rather than an empirical problem that is fatal to the typology as whole. In short, the model assumes the existence of a cline between two general society types.
12. This rendering of a closed society summons Bergson's image of an "instinctive" society, whose ways and structures resembles the social organization of a beehive.
13. The ability to access online information about the Tiananmen Square massacre is vastly different for internet users in China compared with users in the outside world (Kurczy 2010). This is because when leaks of authoritarian government atrocities occur, they are more likely to reach international audiences first.
14. Within this security classification system, the Nazis also implemented organization-specific "Military Secret" and "State Secret" markings –presumably to distinguish certain SS- and Gestapo-originating documents from those that could be disseminated to the military.
15. Noting that early massacres like the Šķēde beach killings were often committed in the open, Holbrook observes that the Nazi party's generally murderous intent was common knowledge across Germany while the Holocaust was being carried out (Holbrook 2023: 388). Nevertheless, the operational and technical specifics of the gas chambers remained a state secret because the system's assembly line-like functioning depended on a deception that victims were being led to "showers" (Sofsky 1993: 260). To the extent that there was contemporaneous external disclosure of the inner horrors of the death camps, the best quality intelligence was mostly provided by survivors. The sole known case of insider whistleblowing about the use of Zyklon B in the camps was Kurt Gerstein, an SS officer who Browning describes as "a covert anti-Nazi" infiltrator (Browning 1999).
16. Trepashkin claimed, credibly, that the weapon was planted by the plain-clothes officers who arrested him (Rodriguez 2004).
17. The most obvious legal manifestation of the transparency principle is seen in Freedom of Information laws, which bestow a citizen right to access government information. Advocates of transparency laws argue that open government reduces corruption, a proposition that has some statistical support in the empirical literature (Kolstad and Wiig 2008, Chen and Ganapati 2021, Parra et al. 2021).
18. Some commentators note that the USA is undergoing "democratic backsliding" and that the rule of law is diminishing (Levitsky & Way 2025). The author agrees with this assessment. However, for the purposes of this analysis, the USA is categorized as an open democracy. This is because as a system, America retains many features of "openness" including reasonable protections for a free press and an at-least partially functional Freedom of Information Act system. The disclaimer is that this openness is potentially subject to rapid change.
19. Subsequent reporting on a similar pattern of war crimes within the UK Special Forces (UKSF) indicates that an influential "code of silence" was also present in 22SAS, the SASR's British sister unit (BBC News 2025).

20. Ben Roberts-Smith, a publicly venerated Victoria Cross recipient, was one of the soldiers involved in the Sola raid, so it is open to infer that this "national interest" related to adverse public affairs fallout. The existence of the Sola Report is now public knowledge thanks to David McBride's unauthorized disclosures.
21. The roll-out of these "Records of Conversation" followed the publication of news reports on war crimes that anonymously quoted confidential sources SASR (*The Age* 2020).
22. Credible information indicates that 2nd Commando Regiment soldiers murdered prisoners in Afghanistan (Willacy et al. 2022, McKenzie & Masters 2021, *Russell v ABC* 2023: 132). In 2021, Russell's platoon was the subject of specific investigation by Australia's Office of the Special Investigator, a war crimes-focused police unit. However, when ABC News later published accusations that Russell was personally involved in unlawful killings himself, Russell successfully sued for defamation (*Russell v ABC* 2023: 144–145).
23. The government did not make the same argument in *Russell v ABC*. Special forces personnel were involved in this case were openly identified.
24. The anonymization of perpetrators and the de-anonymization of the victim community represented an inversion of the identity protection system observed in other types of criminal matters, like sexual assault cases.
25. The Australian state's censorship of perpetrator-identifying information domestically while being unable to prevent the publication of these names abroad resembles the jurisdictional restraints experienced by China in its suppression of Tinanamen-related information. It also resembled a similar affair in Australia during the Cardinal George Pell case. When Pell was convicted for child sex offences, the story was covered by foreign media but suppressed domestically with a non-publication order. Australian newspapers who published the same information were aggressively pursued for contempt of court (Bosland 2022).
26. Using masks is a common criminal tactic, whether for crimes of gain like robbery, or for even more serious offences like hate crimes and terrorism. The Ku Klux Klan's crimes in the post-bellum American South are the paradigm case of how anonymization (in this case, anonymization with a hood) can become a symbol of scalable impunity, enabling further criminal offending. Coincidentally, one of the Roberts-Smith-aligned soldiers involved in the Instagram activity brought a Ku Klux Klan costume to Afghanistan "for a laugh" (McKinnell 2022).
27. Shortly after this prosecution policy was divulged to the Senate committee, the proceedings were rapidly bought to a conclusion by its Chair, a Senator from the party forming government (Commonwealth of Australia 2024, 45–46).
28. Despite being anonymized by a national security suppression order, one soldier asked not to give evidence about "blooding" because he feared the ICC would observe self-incriminating testimony (Federal Court of Australia 2022c)

References

ABC (2017) "The Afghan Files", *ABC News*, 10 July. Available online at: https://www.abc.net.au/news/2017-07-11/killings-of-unarmed-afghans-by-australian-special-forces/8466642 (accessed 20 May 2026).

ABC (2020) "The Killing Field", *ABC News*, 16 March. Available online at: https://www.abc.net.au/news/2020-03-16/killing-field/12060538 (accessed 6 November 2025).

ABC (2023) "The Cost of Speaking Out on Afghanistan", *ABC Radio National Breakfast*, 11 June. Available online at: https://www.abc.net.au/listen/programs/radionational-breakfast/the-cost-of-speaking-out-on-afghanistan/102467716 (accessed 6 November 2025).

ABC (2024) "Years in Jail for Exposing Military Secrets", *ABC News*, 15 May. Available online at: https://www.abc.net.au/listen/programs/abc-news-daily/years-jail-for-exposing-military-secrets/103852412 (accessed 6 November 2025).

Agamben, G. (2005) *State of Exception*. Chicago: University of Chicago Press.

Al Jazeera (2018) "Reuters: Journalists Held for Probing Rohingya Massacre", *Al Jazeera*, 9 February. Available online at: https://www.aljazeera.com/news/2018/2/9/reuters-journalists-held-for-probing-rohingya-massacre (accessed 6 November 2025).

Amnesty International (2022a) "Russia: Navalny Facing Possible 15-Year Jail Term in 'Sham' Trial Set to Take Place in Prison". Available online at: https://www.amnesty.org.uk/press-releases/russia-navalny-facing-possible-15-year-jail-term-sham-trial-set-take-place-prison (accessed 6 November 2025).

Amnesty International (2022b) "Russia: Aleksei Navalny Facing up to 15 Years behind Bars in New 'Sham' Prison Trial". Available online at: https://www.amnesty.org/en/latest/news/2022/02/russia-aleksei-navalny-facing-up-to-15-years-behind-bars-in-new-sham-prison-trial/ (accessed 6 November 2025).

Amnesty International (2024) "Israeli authorities' shutdown of Al Jazeera's Ramallah office a crushing blow for press freedom". Available online at: https://www.amnesty.org/en/latest/news/2024/09/israeli-authorities-shutdown-of-al-jazeeras-ramallah-office-a-crushing-blow-for-press-freedom/ (accessed 6 November 2025).

Anderson, S. (2017) "None Dare Call It a Conspiracy", *GQ*. Available online at: https://www.gq.com/story/moscow-bombings-mikhail-trepashkin-and-putin (accessed 6 November 2025).

AsianLii (1923) "Myanmar Laws: Burma Official Secrets Act, 1923". Available online at: http://www.asianlii.org/mm/legis/laws/bosa1923206/ (accessed 6 November 2025).

Attorney-General's Department (2024) "Senate Legal and Constitutional Affairs Legislation Committee. Criminal Code Amendment (Genocide, Crimes against Humanity and War Crimes) Bill 2024. Attorney-General's Department Submission. July 2024".

Australian Government Solicitor (2020) "Interlocutory Application – Form 35 – Rule 17.01(1)(a)", in *Roberts-Smith v Fairfax Media Publications Pty Ltd*. FCA. Available online at: https://www.fedcourt.gov.au/__data/assets/pdf_file/0008/77831/NSD1485-2018-Interlocutory-Application-972020-145611187.pdf (accessed 6 November 2025).

BBC (2012) "New Powers for Russia's FSB Alarm Rights Activists", *BBC News*, 6 March. Available online at: https://www.bbc.com/news/world-europe-10801029 (accessed 20 May 2026).

BBC (2023) "Top General Locked Away Evidence of SAS Executions", *BBC News*, 16 November. Available online at: https://www.bbc.co.uk/news/uk-67418001 (accessed 06 November 2025).

Beamish, T. (2000) "Accumulating Trouble: Complex Organization, a Culture of Silence, and Secret Spill", *Social Problems*, 47(4): 473–498.

Bergson, H. (1935) *The Two Sources of Morality and Religion*. Notre Dame: University of Notre Dame Press.

Biddle, S. (2016) "Top-Secret Snowden Document Reveals What the NSA Knew about Previous Russian Hacking", *The Intercept*. Available online at: https://theintercept.com/2016/12/29/top-secret-snowden-document-reveals-what-the-nsa-knew-about-previous-russian-hacking/ (accessed 6 November 2025).

Bigg, C. (2006) "Russia: Politkovskaya Investigating Chechen Torture at Time of Death", *Radio Free Europe*. Available online at: https://www.rferl.org/a/1071891.html (accessed 6 November 2025).

Bosland, J. (2022) "Open Justice, 'Back-To-Back' Trials and Juror Prejudice: Examining the Suppression Order in the Trial of George Pell", *Melbourne University Law Review*, 45(2): 462–510.

Botero, G. (2017) *Botero: The Reason of State*. Cambridge: Cambridge University Press.

Brandt, E. (1980) "On Secrecy and the Control of Knowledge: Taos Pueblo", in S. Teft ed. *Secrecy: A Cross-Cultural Perspective*. New York: Human Sciences Press.

Breitman, R. (1996) "Secrecy and the Final Solution", in R. Millen ed. *New Perspectives on the Holocaust: A Guide for Teachers and Scholars*. New York: New York University Press.

Brevini, B. (2017) "Wikileaks: Between Disclosure and Whistle-Blowing in Digital Times", *Sociology Compass*, 11(3): e12457.

Browning, C. (1999) "Day 17 Trial Transcript", *Holocaust Denial on Trial*, Emory University. Available online at: https://www.hdot.org/day17/#:~:text=Kurt%20Gerstein%20was%20a%20covert%20anti%2DNazi (accessed 20 May 2026).

Bump, P. (2019) "Digging into the details of the indictment against Julian Assange", *The Washington Post*, 11 April. Available online at: https://www.washingtonpost.com/politics/2019/04/11/digging-into-details-indictment-against-julian-assange/ (accessed 6 November 2025).

Burnham, D. (1970) "Inquiry on Police Corruption Queries Captain Accused of Abetting Bribery", *New York Times*, 12 November. Available online at: https://www.nytimes.com/1970/11/12/archives/inquiry-on-police-corruption-queries-captain-accused-of-abetting.html (accessed 6 November 2025).

Burnham Inquiry (2020). "Email: External Release Issue, External to the Sitrep". Available online at: https://operationburnham.inquiry.govt.nz/__data/assets/pdf_file/0036/18999/9-191202-0807-external-release-issue-external-to-the-sitrep-updated.pdf. (accessed 20 May 2026).

Cadwalladr, C. (2018) "'I spent seven years fighting to survive': Chelsea Manning on whistleblowing and WikiLeaks", *The Guardian*, 7 October. Available online at: https://www.theguardian.com/us-news/2018/oct/07/chelsea-manning-wikileaks-whistleblowing-interview-carole-cadwalladr (accessed 6 November 2025).

CBC (2010) "Karzai says Wikileaks war logs endanger informants", *CBC News*. Available online at: https://www.cbc.ca/news/world/karzai-says-wikileaks-war-logs-endanger-informants-1.945553 (accessed 6 November 2025).

Chen, C. and Ganapati, S. (2021) "Do Transparency Mechanisms Reduce Government Corruption? A Meta-Analysis", *International Review of Administrative Sciences*, 89(1): 257–272.

Clapmarius, A. (1644) *Conclusiones de jure publico*. Available online at: https://play.google.com/books/reader?id=Z2tEAAAAcAAJ&pg=GBS.PP1&hl=en_US (accessed 6 November 2025).

CNN (1999) "Russian bomb scare turns out to be an anti-terror drill", 24 September. Available online at: http://edition.cnn.com/WORLD/europe/9909/24/russia.bomb.01/ (accessed 20 May 2026).

Commission on Security and Cooperation in Europe (2004) "The Case of Mikhail Trepashkin: Hon Christopher H. Smith, House of Representative, 108th Congress, Second Session". Available online at https://www.csce.gov/statements/case-mikhail-trepashkin/ (accessed 6 November 2025).

Committee to Protect Journalists (2023) "Russia Orders Arrest of Bellingcat Journalist Christo Grozev". Available online at: https://cpj.org/2023/04/russia-orders-arrest-of-bellingcat-journalist-christo-grozev/ (accessed 6 November 2025).

Commonwealth of Australia (2023) "Foreign Affairs, Defence and Trade Legislation Committee", *Proof Committee Hansard – Senate*, 30 May. Available online at: https://www.aph.gov.au/-/media/Estimates/fadt/bud2324/Hansards/1_300523_Defence_PROOF.pdf (accessed 6 November 2025).

Commonwealth of Australia (2024) "Proof Committee Hansard – Senate – Legal and Constitutional Affairs Legislation Committee, Criminal Code Amendment (Genocide, Crimes against Humanity and War Crimes) Bill 2024", 30 July.

Corriere (2010) "La madre del bimbo sciolto nell'acido 'Giuseppe ha vinto, la mafia ha perso'", *Corriere della Sera*, 10 November. Available online at: https://www.corriere.it/cronache/08_novembre_10/di_matteo_mafia_b457bb48-af0c-11dd-bbcd-00144f02aabc.shtml (accessed 6 November 2025).

Costas, J. and Grey, C. (2014) "Bringing Secrecy into the Open: Towards a Theorization of the Social Processes of Organizational Secrecy", *Organization Studies*, 35(1): 1423–1447.

Defence Australia (2023) "FOI 406/22/23". Available online at: https://defence.gov.au/sites/default/files/2023-02/defence_foi_406_22_23_-_document-for-release.pdf (accessed 6 November 2025).

Defence Australia (2025a) "Defence Security Principles Framework (DSPF): Protected Identities". Available online at: https://www.defence.gov.au/sites/default/files/2024-09/Defence%20FOI%20 0084%202425%20-%20Documents%20for%20Release.pdf (accessed 6 November 2025).

Defence Australia (2025b) "FOI 291/25/26". Available online at: https://www.defence.gov.au/sites/default/files/2025-10/Defence-FOI-291_25_26-Documents.pdf (accessed 6 November 2025).

DeMaria, W. (2006) "Brother Secret, Sister Silence: Sibling Conspiracies against Managerial Integrity", *Journal of Business Ethics*, 65: 219–234.

Doherty, B. (2022a) "Ben Roberts-Smith Defamation Trial: Witness Tells Court He Liked Instagram Post Calling Dead Afghan a 'Terrorist Paedo'", *The Guardian*, 28 April. Available online at: https://www.theguardian.com/australia-news/2022/apr/28/ben-roberts-smith-defamation-trial-witness-tells-court-he-liked-instagram-post-calling-dead-afghan-a-terrorist-paedo (accessed 6 November 2025).

Doherty, B. (2022b) "Australian Special Forces Member Allegedly Stole and Published Personal Data of Intelligence Official", *The Guardian*, 18 November. Available online at: https://www.theguardian.com/australia-news/2022/nov/18/australian-special-forces-member-allegedly-stole-and-published-personal-data-of-intelligence-official (accessed 6 November 2025).

Elian, A. and Cliteur, P. (2021) *The Open Society and Its Closed Communities*. The Hague: Eleven International Publishing.

Federal Court of Australia (2022a) "Respondents' Witness List", in *Roberts-Smith v Fairfax Media Publications Pty Ltd*. Available online at: https://www.fedcourt.gov.au/services/access-to-files-and-transcripts/online-files/ben-roberts-smith/Respondents-Witness-List.pdf (accessed 6 November 2025).

Federal Court of Australia (2022b) *Roberts-Smith v Fairfax Media Publications Pty Ltd (No 34)* [2022] FCA 532. Available online at: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2022/2022fca0532 (accessed 6 November 2025).

Federal Court of Australia (2022c) *Roberts-Smith v Fairfax Media Publications Pty Ltd (No 40)* [2022] FCA 1614. Available online at: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2022/2022fca1614 (accessed 6 November 2025).

Ferencz, B. (1999) "A Prosecutor's Personal Account – Nuremberg to Rome". Available online at: https://benferencz.org/articles/1990-1999/a-prosecutors-personal-account-nuremberg-to-rome/ (accessed 6 November 2025).

Felshtinsky, Y. and Litvinenko, A. (2002) *Blowing up Russia: Terror from Within*. New York: SPI Books.

Government of Canada. (2024) "Government of Canada Trust and Transparency Strategy". Available online at: https://www.canada.ca/en/government/system/government-wide-reporting-spending-operations/trust-transparency/government-canada-trust-and-transparency-strategy.html (accessed 6 November 2025).

Graham-Harrison, E. (2025) "Israel's Top Military Lawyer Arrested after She Admitted Leaking Video of Soldiers' Abuse", *The Guardian*, 3 November. Available online at: https://www.theguardian.com/world/2025/nov/03/israels-top-military-lawyer-arrested-after-she-admitted-leaking-video-of-soldiers-abuse (accessed 6 November 2025).

Hammersley, M. (2024) "What Is an 'Open Society'? Bergson, Strauss, Popper, and Deleuze", *History of European Ideas*, 50(8): 1422–1432.

Head, J. (2017) "Myanmar's 'Drastic' Arrest of Journalists Causes Concern", *BBC News*, 21 December. Available online at: https://www.bbc.com/news/world-asia-42437085 (accessed 6 November 2025).

Hedges, C. (1998) "Threats Worry 3 Who Tied Croatian Army to Atrocities", *New York Times*, 15 February. Available online at https://www.nytimes.com/1998/02/15/world/threats-worry-3-who-tied-croatian-army-to-atrocities.html (accessed 6 November 2025).

Hiatt, L. (1971) "Secret Pseudo-Procreating Rites among the Australian Aborigines", in L. Hiatt and C. Jayawardena eds. *Anthropology in Oceania: Essays Presented to Ian Hogbin*. Sydney: Angus & Robertson.

Holbrook, M. (2023) *Bystander Society: Conformity and Complicity in Nazi Germany and the Holocaust*. Oxford: Oxford University Press.

Horn, E. (2011) "Logics of Political Secrecy", *Theory, Culture and Society*, 28(7–8): 103–122.

Human Rights Law Centre (2025) "Tax Whistleblower Richard Boyle's Guilty Plea and Indictment on Australia's Broken Whistleblowing Laws". Available online at: https://www.hrlc.org.au/news/tax-whistleblower-richard-boyle-guilty-plea/ (accessed 6 November 2025).

Human Rights Watch (2006) "Soldiers' Accounts". Available online at: https://www.hrw.org/reports/2006/us0706/2.htm (accessed 6 November 2025).

Independent Inquiry relating to Afghanistan (2024) "YouTube: Day12 AM – IIA Witnesses – Rt Hon Johnny Mercer MP & Mark Nicol. Timestamp: 2:17:38–2:19:15". Available online at: https://youtu.be/m8GJGONhYB4?t=8244 (accessed 6 November 2025).

Independent Inquiry relating to Afghanistan (2025) "MOD-198-0001586-A. Op A Security Compartment". Available online at: https://iiaweb-prod.s3.eu-west-2.amazonaws.com/MOD-198-0001586-A.pdf (accessed 6 November 2025).

International Criminal Court Act [Aus] (2002) "Commonwealth Consolidated Acts". Available online at: https://www.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/icca2002303/ (accessed 6 November 2025).

Inspector General of the Australian Defence Force (2020a) "Inspector General of the Australian Defence Force Afghanistan Inquiry", *Department of Defence*, 6 November. Available online at: https://www.defence.gov.au/sites/default/files/2021-10/IGADF-Afghanistan-Inquiry-Public-Release-Version.pdf (accessed 6 November 2025).

Inspector General of the Australian Defence Force (2020b) "Affidavit – Form 49 – Rule 29.02(1)", in *Roberts-Smith v Fairfax Media Publications Pty Ltd*. FCA. Available online at: https://www.fedcourt.gov.au/__data/assets/pdf_file/0008/79118/Affidavit-of-Fiona-Sneath-sworn-7-August-2020.pdf (accessed 6 November 2025).

International Criminal Court Act [UK] (2001) "Section 39". Available online at https://www.legislation.gov.uk/ukpga/2001/17/section/39 (accessed 6 November 2025).

International Criminal Tribunal for Yugoslavia (2000) "Press Release: Office of the Prosecutor: Reported Murder of Milan Levar in Croatia". Available online at: https://www.icty.org/en/press/reported-murder-milan-levar-croatia (accessed 6 November 2025).

Kleinig, J. (2001) "The Blue Wall of Silence: An Ethical Analysis", *International Journal of Applied Philosophy*, 15(1): 1–23. Available online at: https://www.researchgate.net/profile/John-Kleinig/publication/269738281_The_Blue_Wall_of_Silence/links/56f35cc508ae38d7109a58a9/The-Blue-Wall-of-Silence.pdf (accessed 06 November 2025).

Kolstad, I. and Wiig, A. (2008) "Is Transparency the Key to Reducing Corruption in Resource-Rich Countries?", *World Development*, 37(3): 521–532.

Kurczy, S. (2010) "Tiananmen Square Massacre Now Searchable on Google China?", *The Christian Science Monitor*, 16 March. Available online at: https://www.csmonitor.com/World/Global-News/2010/0316/Tiananmen-Square-massacre-now-searchable-on-Google-China (accessed 6 November 2025).

Levitsky, S. and Way, L. (2025) "The Path to American Authoritarianism: What Comes after Democratic Breakdown", *Foreign Affairs*. Available online at: https://www.foreignaffairs.com/united-states/path-american-authoritarianism-trump (accessed 6 November 2025).

Lone, W., Soe Oo, K., Lewis, S., and Slodkowski, A. (2018) "How Myanmar forces burned, looted and killed in a remote village", *Reuters*. Available online at: https://www.reuters.com/investigates/special-report/myanmar-rakhine-events/ (accessed 6 November 2025).

Maccharles, T. (2006) "'Secret' Soldier Can't Be Charged", *The Star*. Available online at: https://web.archive.org/web/20070929105754/http://www.thestar.com/News/article/164279 (accessed 6 November 2025).

Manderson, L., Davis, M., Colwell, C. and Ahlin, T. (2015) "On Secrecy, Disclosure, the Public and the Private in Anthropology: An introduction to Supplement 12", *Current Anthropology*, 56(Supplement 12): s183–190.

McHugh, F. (2025) "Years after It Was Exposed, Defence Has Closed a Serious Database Loophole", *Capital Brief*, 8 January. Available online at: https://www.capitalbrief.com/article/years-after-it-was-exposed-defence-has-closed-a-serious-database-loophole-9c918b40-4d01-4981-a9b7-afe75fe3f890/ (accessed 6 November 2025).

McKenzie, N. and Masters, C. (2021) "As Australia's War Crimes Investigations Drag On, Misinformation Is Catching", *The Age*, 26 August. Available online at: https://www.theage.com.au/national/as-australia-s-war-crimes-investigations-drag-on-misinformation-is-catching-up-20210826-p58m31.html (accessed 6 November 2025).

McKenzie, N. (2023) "War Crimes Investigators Narrow Focus to Three Key Targets, Including Roberts-Smith", *Sydney Morning Herald*, 18 January. Available online at: https://www.smh.com.au/national/war-crimes-investigators-narrow-focus-to-three-key-targets-including-roberts-smith-20230118-p5cdge.html (accessed 6 November 2025).

McKinnell, J. (2022) "Ben Roberts-Smith Witness Won Fancy Dress Competition Wearing White Supremacist Outfit, Court Told", *ABC News*, 28 April. Available online at: https://www.abc.net.au/news/2022-04-28/ben-roberts-smith-witness-won-competition-dressed-as-klansman/101022224 (accessed 6 November 2025).

Mediazona (2023) "Mediazona publisher Pyotr Verzilov arrested in absentia in military 'fakes' case over posts about Bucha killings". Available online at: https://zona.media/news/2023/03/27/verzilov (accessed 18 May 2026).

Meduza (2023) "Pyotr Verzilov, Mediazona Founder and Pussy Riot Spokesperson Charged with Distributing 'Fakes' about the Russian Army". Available online at: https://meduza.io/amp/en/news/2023/01/26/pyotr-verzilov-mediazona-founder-and-pussy-riot-spokesperson-charged-with-distributing-fakes-about-the-russian-army (accessed 20 May 2026).

Murphy, K. (2004) "Russian ex-agent's sentencing called political", *Los Angeles Times*, 20 May. Available online at: https://www.latimes.com/archives/la-xpm-2004-may-20-fg-agent20-story.html (accessed 6 November 2025).

Myanmar Now (2019) "Army Soldiers Who Committed Inn Din Village Massacre Released before Serving a Year in Prison". Available online at: https://myanmar-now.org/mm/news/2133/?tztc=1 (accessed 6 November 2025).

Naing, S. and Lewis, S. (2019) "Myanmar's top court rejects final appeal by jailed Reuters journalists", *Reuters*, 23 April. Available online at: https://www.reuters.com/article/us-myanmar-journalists/myanmars-top-court-rejects-final-appeal-by-jailed-reuters-journalists-idUSKCN1RZ06O/(accessed 6 November 2025).

Naing, S. and Slodkowski, A. (2018) "Myanmar police 'set up' Reuters reporters in sting – police witness", *Reuters*, 20 April. Available online at: https://www.reuters.com/article/us-myanmar-journalists/myanmar-police-set-up-reuters-reporters-in-sting-police-witness-idUSKBN1HR12Q/(accessed 6 November 2025).

National Center for Victims of Crime (2007) "'Snitches get Stitches': Youth, Gangs and Witness Intimidation in Massachusetts". Available online at: https://victimsofcrime.org/doc/Snitches%20FINAL.pdf (accessed 6 November 2025).

National Defence (2022) "DAOD 2006-1. 4(4.2). Procedures for the Safeguarding and Authorized Disclosure of Information in the DND and the CAF". Available online at: https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/2000-series/2006/2006-1-procedures-safeguarding-authorized-disclosure-information.html (accessed 6 November 2025).

New York Times (NYT). (1970) "Police Use Own Words to Speak of Corruption", *New York Times*, 25 April. Available online at: https://www.nytimes.com/1970/04/25/archives/police-use-own-words-to-speak-of-corruption.html (accessed 6 November 2025).

Nuremberg Military Trial 4 (1947) "Transcript for NMT 4: Pohl Case", *Harvard Law Society Nuremberg Trials Project*. Available online at: https://nuremberg.law.harvard.edu/transcripts/5-transcripts-for-nmt-4-pohl-case (accessed 6 November 2025).

Nuremberg Military Trial 7 (1947) "Transcript for NMT 7: Hostage Case", *Harvard Law Society Nuremberg Trials Project*. Available online at: https://nuremberg.law.harvard.edu/transcripts/4-transcript-for-nmt-7-hostage-case (accessed 6 November 2025).

NZ Protective Security. (2022) "New Zealand Government Information Security Classification System Policy 2022". Available online at: https://protectivesecurity.govt.nz/assets/Classification/Classification-System-Policy-2022.pdf (accessed 06 November 2025).

Office of the High Commissioner for Human Rights (1998) Rome Statute of the International Criminal Court. United Nations. https://www.ohchr.org/en/instruments-mechanisms/instruments/rome-statute-international-criminal-court

Office of the Director of National Intelligence (2016) *Improving the Intelligence Community's Declassification Process and the Community's Support to the National Declassification Center*. Available online at: https://sgp.fas.org/othergov/intel/improving.pdf (accessed 6 November 2025).

Owen, R. (2016) *The Litvinenko Inquiry: Report into the Death of Alexander Litvinenko*. London: Her Majesty's Stationery Office. Available online at: https://assets.publishing.service.gov.uk/media/5a8055c340f0b62302692e48/The-Litvinenko-Inquiry-H-C-695-web.pdf (accessed 6 November 2025).

Paoli, L. (2003) *Mafia Brotherhoods: Organized Crime, Italian Style*. Oxford: Oxford University Press.

Parliament of Australia (2023) "Petition EN4991 – Protected Identity for Our Veterans & Their Families". Available online at: https://www.aph.gov.au/e-petitions/petition/EN4991 (accessed 6 November 2025).

Parra, D., Muñoz-Herrera, M., and Palacio, L. (2021) "The Limits of Transparency in Reducing Corruption", *Journal of Behaviour and Experimental Economics*, e101762.

PEN America (2019) "Myanmar Supreme Court's Decision to Uphold Convictions of Reuters Journalists Wa Lone and Kyaw Soe Oo a Devastating Blow", *PEN America*. Available online at: https://pen.org/press-release/myanmar-supreme-court-upholds-conviction-wa-lone-kyaw-soe-oo/ (accessed 6 November 2025).

Pender, K. and Greste, P. (2024) "The Jailing of David McBride Is a Dark Day for Democracy and Press Freedom in Australia", *The Guardian*, 14 May. Available online at: https://www.theguardian

.com/media/commentisfree/article/2024/may/14/the-jailing-of-david-mcbride-is-a-dark-day-for-democracy-and-press-freedom-in-australia (accessed 6 November 2025).

Plato [translated by Jowett, B.]. (1991) *The Republic: The Complete & Unabridged Jowett Translation*. New York: Vintage Books.

Politkovskaya, A. (2004) "Poisoned by Putin", *The Guardian*, 9 September. Available online at: https://www.theguardian.com/world/2004/sep/09/russia.media (accessed 6 November 2025).

Politkovskaya, A. (2006) "Poison in the air", *The Guardian*, 1 March. Available online at: https://www.theguardian.com/world/2006/mar/01/russia.chechnya (accessed 6 November 2025).

Pope, H. (2024) "US Hits Accountants Tied to Cartel Fraud Scheme", *Organized Crime and Corruption Reporting Project*. Available online at: https://www.occrp.org/en/news/us-hits-accountants-tied-to-cartel-fraud-scheme (accessed 6 November 2025).

Popper, K. (1994) *The Open Society and Its Enemies*. Princeton: Princeton University Press.

Prima News (2004) "State Secret Disclosed in the Book about Terrorist Acts". Available online at: https://web.archive.org/web/20110823155844/http://old.prima-news.ru/eng/news/news/2004/1/30/27326.html (accessed 6 November 2025).

PSPF (2023) "Policy 8: Sensitive and Security Classified Information". Available online at https://webarchive.nla.gov.au/awa/20210603072457/https://www.protectivesecurity.gov.au/information/Pages/default.aspx (accessed 20 May 2026).

R v McBride (2024) ACT Supreme Court. Available online at: https://www.courts.act.gov.au/__data/assets/pdf_file/0003/2451369/McBride-No-4.pdf (accessed 06 November 2025).

Reuters. (2018) "Reuters statement on jailed reporters Wa Lone and Kyaw Soe Oo, Aug 20", 20 August. Available online at: https://www.reuters.com/article/rpb-reutersstatemnetaug20/reuters-statement-on-jailed-reporters-wa-lone-and-kyaw-soe-oo-aug-20-idUSKCN1L50IJ/ (accessed 6 November 2025).

Richardson, D. (2019) "Comprehensive Review of the Legal Framework of the National Intelligence Community". Available online at: https://www.ag.gov.au/system/files/2020-12/volume-3-information-technology-powers-and-oversight.PDF (accessed 6 November 2025).

Rimington, H. (2022) "@hughriminton, 29 Apr 2022: The #BenRobertsSmith trial has just gone into closed court", *Twitter*. Available online at: https://x.com/hughriminton/status/1519918630598692864 (accessed 6 November 2025).

Rodriguez, A. (2004) "Chicago Tribune follows Trepashkin's trail", *Prima News*, 19 May. Available online at: https://web.archive.org/web/20111007033726/http://old.prima-news.ru/news/news/2004/5/19/28486.html (accessed 6 November 2025).

Roskomsvoboda (2018) "Satellite Internet vs FSB: Technological Development or Self-Isolation?". Available online at: https://roskomsvoboda.org/en/42992/ (accessed 6 November 2025).

Russian Federation. (1995) "Law of the Russian Federation No.5485-1 of July 21, 1993 on State Secrets", *World Trade Organization Legal Database*. Available online at: https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_125.pdf (accessed 6 November 2025).

Russian Federation. (2012) "Federal Law of the Federal Security Service of the Russian Federation", Council of Europe translation. Available online at: https://policehumanrightsresources.org/content/uploads/2016/08/Federal-Law-on-Federal-Security-Service-Russia-1995.pdf?x96812 (accessed 6 November 2025).

Russell v ABC (2023) FCA 1223. Available online at: https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2023/2023fca1223 (accessed 6 November 2025).

Sagar, R. (2023) *Secrets and Leaks: The Dilemma of State Secrecy*. Princeton, NJ: Princeton University Press.

Special Broadcasting Service (2023) "'Code of Silence': Did the ADF threaten a Ben Roberts-Smith witness with criminal charges?". Available online at: https://www.sbs.com.au/news/article/code-of-silence-did-defence-threaten-a-ben-roberts-smith-witness-with-criminal-charges/g65sit5db (accessed 6 November 2025).

Schmidt, M. (2013) "Ex-CIA Officer Sentenced to 30 Months in Leak", *New York Times*, 26 January. Available online at: https://www.nytimes.com/2013/01/26/us/ex-officer-for-cia-is-sentenced-in-leak-case.html (accessed 6 November 2025).

Schmitt, C. (1985) *Political Theology: Four Chapters on the Concept of Sovereignty* (trans. G. Schwab). Chicago: University of Chicago Press.

Sereny, G. (1974) *Into that Darkness*. New York: Vintage Books.

Shoebridge, D. (2025) "@davidshoebridge, 25 Feb 2025: $2,676,820 is a lot to spend prosecuting a whistleblower", *Twitter*. Available online at: https://x.com/DavidShoebridge/status/1894272853891322081 (accessed 6 November 2025).

Simmel, G. (1906) "The Sociology of Secrecy and of Secret Societies", *American Journal of Sociology*, 11(4): 441–498.

Smith, R. J. (2000) "Death of a Man Who Knew Too Much", *The Washington Post*, 14 September. Available online at: https://www.washingtonpost.com/archive/politics/2000/09/14/death-of-a-man-who-knew-too-much/71ad72a3-eb4c-4f76-8a9e-f7bb845311d9/ (accessed 6 November 2025).

Snow, D. (2003) "Army Clears SAS Soldier", *Sydney Morning Herald*, 1 October. Available online at: https://www.smh.com.au/world/asia/army-clears-sas-soldier-20031001-gdhi42.html (accessed 6 November 2025).

Sofsky, W. (1993) *The Order of Terror: The Concentration Camp*. Frankfurt: Fischer.

Sydney Morning Herald (2023) "Stick to the Code: New Tapes Reveal Ben Roberts-Smith's Campaign to Silence Soldiers". Available online at: https://www.smh.com.au/national/stick-to-the-code-new-tapes-reveal-ben-roberts-smith-s-campaign-to-silence-soldiers-20230411-p5czj2.html (accessed 6 November 2025).

Teft, S. (1980) "Introduction", in S. Teft ed. *Secrecy: A Cross-Cultural Perspective*. New York: Human Sciences Press.

The Age (2020) "Special Forces Chief Acknowledges War Crimes, Blames 'Poor Moral Leadership'". Available online at: https://www.theage.com.au/national/special-forces-chief-acknowledges-war-crimes-blames-poor-moral-leadership-20200628-p556z6.html (accessed 6 November 2025).

The Guardian (2010) "Afghanistan war logs: Polish attack on village kills five, wounds several, including pregnant woman at wedding party". Available online at: https://www.theguardian.com/world/afghanistan/warlogs/5EA14116-2B6B-470C-8DB4-2912DDF197BF (accessed 6 November 2025).

Treasury Board Secretariat Canada (2019) "Rescinded [2019-06-28] – Security Organization and Administration Standard". Available online at: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=12333&section=html (accessed 6 November 2025).

Tushnet, M. and Bugaric, B. (2022) *Power to the People: Constitutionalism in the Age of Populism*. New York: Oxford Academic.

UK Ministry of Defence. (2023) "Joint Doctrine Publication 2-00: Intelligence, Counter-Intelligence and Security Support to Joint Operations". Available online at: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf (accessed 20 May 2026).

United Nations. (2024) "Russia: UN Human Rights Office 'Appalled' at Death of Navalny in Prison". Available online at: https://news.un.org/en/story/2024/02/1146627 (accessed 6 November 2025).

US National Archive (2009) "The President Executive Order 13526. Classified National Security Information". Available online at: https://www.archives.gov/isoo/policy-documents/cnsi-eo.html #six (accessed 6 November 2025).

Usher, S. (2025) "Israeli military's top lawyer resigns over leak of video allegedly showing abuse of Palestinian detainee", *BBC News*, 3 November. Available online at: https://www.bbc.com/news /articles/cy0kpd97qqko (accessed 6 November 2025).

Verzilov, P. (2022a) "@petyaverzilov, 3 Apr 2022: What happened in Bucha is one of the monstrous crimes of the 21st century", *Instagram*. Available online at: https://www.instagram.com/p /Cb5uIAQLN0q/?hl=ru (accessed 6 November 2025).

Verzilov, P. (2022b) "@petyaverzilov, 14 Apr 2022: the yard of the house in Bucha", *Instagram*. Available online at: https://www.instagram.com/tv/CcVq8yJFI-i/ (accessed 6 November 2025).

Verzilov, P. (2022c) "@grupp_voina, 8 Apr 2022: Standing today by the mass grave in Bucha", *Twitter*. Available online at: https://x.com/gruppa_voina/status/1512518811735441423 (accessed 6 November 2025).

Verzilov, P. (2022d) "@gruppa_voina, 8 Apr 2022: Russian soldiers who did this in Bucha", *Twitter*. Available online at: https://x.com/gruppa_voina/status/1512498505906020355 (accessed 6 November 2025).

Veteran Support Force. (2023) "VSF Petition 'Protected Identity for Our Veterans & Their Families'". Available online at: https://rarnational.org.au/vsf-petition-protected-identity-for-our-veterans-their -families/ (accessed 6 November 2025).

Westmarland, L. (2013) "'Snitches Get Stitches': US Homicide Detectives' Ethics and Morals in Action", *Policing and Society*, 23(3): 311–327.

Westmarland, L and Conway, S. (2020) "Police ethics and integrity: Keeping the 'blue code of silence'", *International Journal of Police Science and Management*, 22(4): 387–392

Werner, D. (1981) "Gerontocracy among the Mekranoti of Central Brazil", *Anthropological Quarterly*, 54(1): 15–27.

Willacy, M., McDonald, A., and Robertson, J. (2022) "Former Australian Commando under Investigation over 2012 Afghanistan Rotation", *ABC News*, 21 September. Available online at: https://www.abc.net.au/news/2022-09-21/australian-commando-under-investigation-over-2012 -rotation/101442434 (accessed 6 November 2025).

Worthy, B. (2017) *The Politics of Freedom of Information: How and Why Governments Pass Laws that Threaten their Power*. Manchester: Manchester University Press.

Zifcak, S. (2020) "Why Bernard Collaery's Case Is One of the Gravest Threats to Freedom of Expression", *Law Society Journal*. Available online at: https://lsj.com.au/articles/why-bernard -collaerys-case-is-one-of-the-gravest-threats-to-freedom-of-expression/(accessed 6 November 2025).